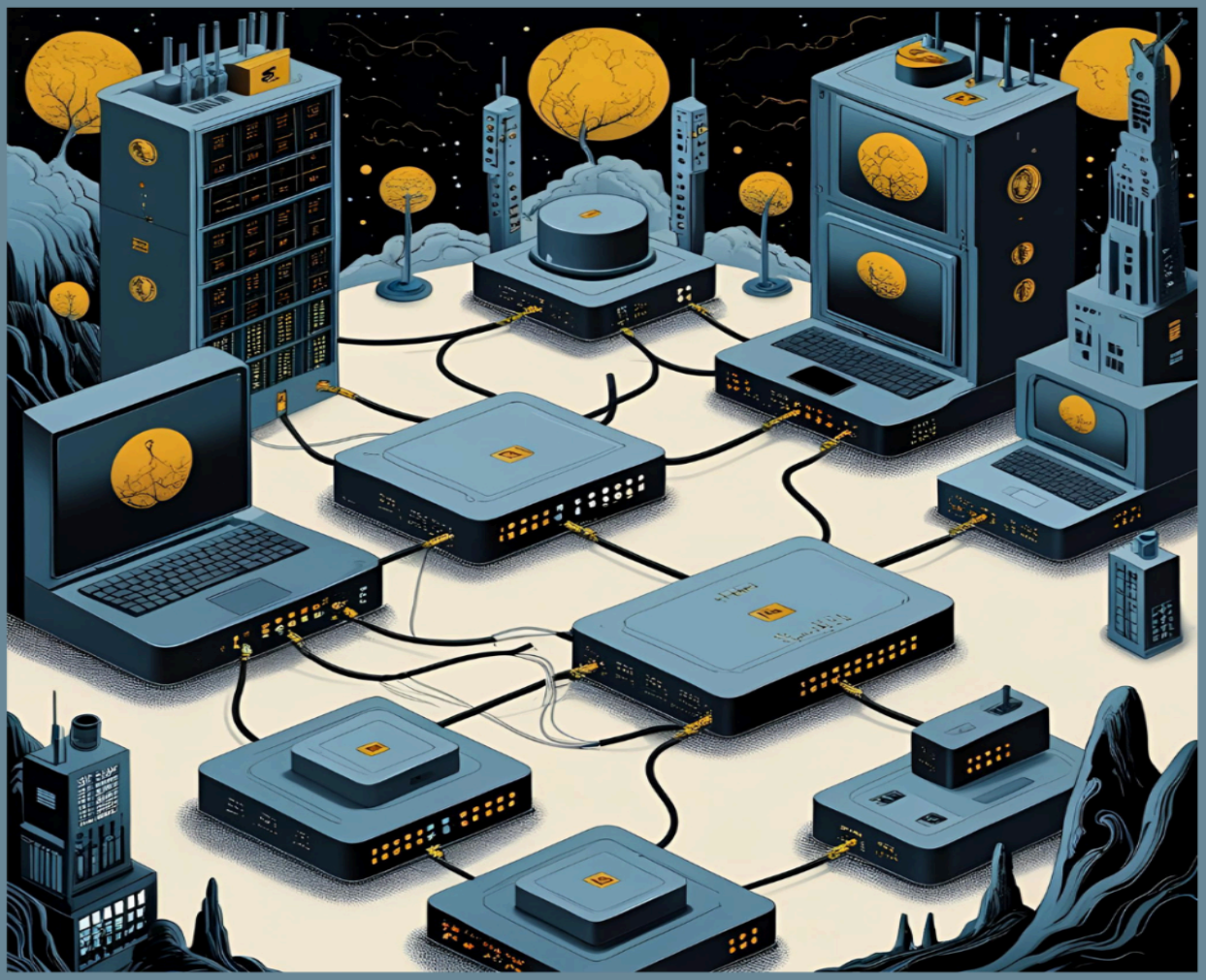
Administração de Switches Gerenciáveis

Um guia prático para switching



EDUARDO MAROÑAS MONKS

Administração de Switches Gerenciáveis

Um guia prático para switching

Eduardo Maroñas Monks

ISBN: 978-65-01-62652-9

2025

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Dedicatória

Dedico este livro a minha família, em especial a minha esposa Vanessa e ao meu filho Gregory, aos meus pais, Pedro e Maria, aos meus amigos e colegas que estiveram e estão comigo dando o apoio para seguirmos em frente trilhando novos caminhos e desafios.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Sumário

Sobre o Autor **8**
Sobre esta Obra **9**
Introdução **10**
1) Conceitos Básicos **13**
1.1 Redes de Computadores 13
1.2 Modelos de Referência OSI 13
1.3 Modelo TCP/IP 16
1.3 Pacotes 17
1.4 Interface de Rede 19
1.5 Endereço Fìsico (MAC Address) 24
1.6 Dispositivos de Rede 26
1.7 Ethernet (IEEE 802.3) 28
1.8 Cabeamento 31
1.9 Conectores 32
1.10 Hubs 36
1.11 Bridges 38
1.12 Switches 39
1.13 Switches Gerenciáveis 41
2) Instalação Física **45**
2.1 Acesso a Porta de Console 46
2.2 Conexão Serial 47
2.3 Solução de Problemas Comuns 51
2.4 Tipos de Cabo 52
2.5 Configurações de Fábrica 53
2.6 Interface de Gerenciamento 54
2.7 Acesso remoto 56
Telnet 56
SSH (Secure Shell) 56
Web GUI (Graphical User Interface) 57
Outras alternativas 57
2.8 Leds de Indicação 58
2.9 Identificação das portas 59
2.10 Racks 60
2.11 Considerações para a Instalação Física de Switches 63

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

2.12 Ferramentas auxiliares....64
3) Configurações Básicas....67
3.1 Nome (Hostname)....67
3.2 Data e Horário....69
3.3 Portas Metálicas....70
Características....71
Estatísticas....71
3.4 Portas de Fibra Óptica....73
Características....74
Estatísticas....75
3.5 Agente SNMP....77
3.6 Logs....79
3.7 Tabela MAC....81
3.8 LLDP (Link Layer Discovery Protocol)....84
3.9 Controles de Tráfego Broadcast e Multicast....86
3.10 Salvar a configuração....89
3.11 Backup/Restore....90
3.12 Atualização de Software (Firmware)....94
3.13 Protocolos de Acesso Remoto....98
3.14 Usuários....102
3.15 Ferramentas de Diagnóstico....105
3.16 Reboot/Reset to Factory Defaults....107
4) VLAN (Virtual LAN)....111
4.1 Primeiro Padrão Formal (IEEE 802.1Q)....112
4.2 Avanços e Adições aos Padrões de VLAN....113
4.3 Interconexão de VLANs....114
4.4 Conceitos Relacionados que Ampliaram as Capacidades das VLANs....116
4.5 Aplicação Prática de VLANs em Redes Corporativas....117
4.6 Estudo de Caso: Empresa ACME....121
5) Configurações Avançadas....129
5.1 Agregação de portas (Link Aggregation)....129
5.2 Espelhamento de Portas (Port MIrroring/SPAN)....134
5.3 STP (Spanning-Tree Protocol)....138
5.4 DHCP Snooping....144
5.5 IGMP Snooping....148
5.6 Loop Detection....151
5.7 ACL (Access Control List)....154
5.8 Limitação de Acesso em Portas (Port Security)....158

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

5.9 QoS (Quality of Service)....162
5.10 Monitoramento de Recursos....166
5.11 Autenticação de Dispositivos....168
5.12 Layer 3....175
6) Cenários de Aplicação....180
6.1 Implementação de VLANs....180
6.2 Ativação de dispositivos VoIP....186
6.3 Cascatemento (Uplink)....188
6.4 Topologia em Anel....192
7) Resolução de Problemas....196
7.1 Busca de Dispositivos....196
7.2 VLAN não funciona....199
7.3 Loops....202
7.4 Anomalias....206
7.5 Adição de Novos Switches....207
7.6 Ferramentas de Gerenciamento....210
7.7 Ferramentas de Simulação e Emulação....214
7.8 Boas Práticas....219
Considerações Finais....222
Referências Bibliográficas....225

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Sobre o Autor

Possui graduação em Bacharel em Análise de Sistemas pela Universidade Católica de Pelotas (1998), Mestrado em Computação pela Universidade Federal do Rio Grande do Sul (2006) e Doutorado pela Universidade Federal de Pelotas (2023). Começou a atuar na área de redes em 1995 como estagiário na UCPEL, onde trabalhou por 14 anos. No período de 1999 a 2004 e 2006 a 2007, atuou como docente em cursos de Ciência da Computação e Tecnologia em Análise e Desenvolvimento de Sistemas na UCPEL. Em 2007, passou a exercer a função de docente da UniSenac Pelotas, em que esteve na coordenação da criação do curso superior em Redes de Computadores, curso que atingiu a nota máxima no ENADE de 2017. Em 2014 tornou-se Analista de TI na UFPEL, atuando na administração de redes. Possui certificados Cisco CCAI, Cisco CCNA e LPIC-1.

Para saber mais: Canal do Youtube criado em 2009 com mais de 600 vídeos sobre a área de redes, disponível em **http://www.youtube.com/emmonks**

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Aviso Importante

Sobre esta Obra

Este livro pode ser usado de forma livre, desde que os créditos e as referências sejam publicados. As informações contidas no documento são de minha autoria, fruto de experiências de mais de 25 anos atuando na área. Nos casos em que são apontadas ferramentas ou sites, poderá haver inconsistências no acesso futuro e poderão causar indisponibilidades.

Se este material tiver ajudado de alguma forma, por favor, contribua com o valor que achar justo como forma de agradecimento, um cafezinho está ótimo. Obrigado!

Chave do PIX: **7f7fa84a-6ce9-45da-a42f-a77d18eb232c**

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Introdução

Este livro tem como objetivo disponibilizar um guia prático para administração de switches gerenciáveis. Os switches são dispositivos fundamentais em qualquer rede local corporativa e possuem funcionalidades importantes para a administração de redes de computadores. O termo *switching* engloba o projeto, a instalação, configuração e administração de switches gerenciáveis. Os switches gerenciáveis oferecem recursos avançados de configuração e monitoramento, permitindo que sejam otimizados o desempenho, a segurança e a disponibilidade da rede.

O começo das redes locais nos anos 80 com o padrão Ethernet (IEEE 802.3), inicialmente com o uso de apenas cabos coaxiais e conversores para as conexões entre os computadores, passando pela evolução do cabeamento para par trançado e a possibilidade do uso de hubs, evoluindo para as pontes (*bridges*) e chegando nos switches evoluíram com o aumento de computadores nas corporações. Um dos fatores mais importantes nesta evolução foi a possibilidade de concentrar as conexões de rede em um equipamento, primeiro com hubs e depois com os switches, e tornar a administração das conexões na rede local gerenciáveis. Posteriormente, com o advento da comutação de pacotes introduzida nas *bridges* e depois nos switches melhorou exponencialmente o desempenho das redes corporativas.

Estas mudanças levaram um tempo considerável para se tornarem o padrão no mercado e chegarem em redes de menor porte. A mudança no uso dos cabos coaxiais, para o uso de cabos do tipo par trançado com hubs, foi motivada pelo aumento do número de computadores nas redes locais. O próximo avanço foi melhorar o desempenho segmentando a rede fazendo o isolamento dos domínios de colisões com o uso de *bridges* (pontes). As *bridges* funcionam fazendo a seleção de quais pacotes devem ser repassados de acordo com os endereços das interfaces de rede.

A funcionalidade de isolar domínios de colisões foi um grande avanço em relação ao uso de hubs repetidores que apenas repetem o sinal e repassam os pacotes sem filtro algum. O hardware de uma *bridge* deve possuir um processamento e memória para realizar a comutação, o que tornou os equipamentos com custo elevado no início. Os switches são a evolução da tecnologia de comutação de pacotes sendo compostos por várias portas que fazem o papel de múltiplas *bridges*. Da mesma forma que as *bridges*, os switches operam na camada 2 (camada de enlace de dados) do modelo OSI. Os switches mantêm uma tabela de

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

endereços MAC, que mapeia os endereços dos dispositivos conectados às suas respectivas portas. Quando um pacote de dados chega a um switch, ele examina o endereço MAC de destino e consulta sua tabela para determinar a porta de saída correta. Esse processo de encaminhamento inteligente permite que os switches criem conexões dedicadas entre dispositivos, reduzindo a colisão de pacotes e aumentando a eficiência da rede.

No final dos anos 90 tornou-se mais acessível a aquisição de switches e havia a necessidade da melhoria considerável no desempenho da rede. Entretanto, ainda havia um grande número de hubs em uso e a substituição destes dispositivos foi sendo realizada de forma gradual. Nesta época ainda era muito raro haver switches gerenciáveis devido ao alto custo. Portanto, os switches não possuíam gerenciamento e a configuração era baseada em conectar os cabos nas portas e observar os leds disponíveis fisicamente nos equipamentos.

Nos anos 2000, com o aumento na quantidade de dispositivos conectados nas redes locais tornou-se crítico o gerenciamento e a administração de forma remota dos switches. Um maior número de fabricantes passaram a oferecer funcionalidades em seus equipamentos para tornar o gerenciamento mais simples e centralizado, o que tornou o custo dos switches gerenciáveis menor. Esta tendência seguiu nas últimas décadas com switches melhores e com maior capacidade, fazendo com que fosse possível substituir todos os hubs e switches não gerenciáveis por dispositivos com gerenciamento.

Porém, as formas de gerenciamento não tinham um padrão entre os fabricantes. Desta forma, com a inevitável diversidade de fabricantes e modelos de switches, tornou-se complexo a administração de switches gerenciáveis em redes corporativas. Mesmo que existam padrões e protocolos que devem ser respeitados por todos os fabricantes, tais como SNMP (*Simple Network Management Protocol*). LLDP (*Link Layer Discovery Protocol*) e STP (*Spanning-Tree Protocol*), os consoles de gerenciamento possuem formas proprietárias para execução de comandos e realização de configurações. As consoles de gerenciamento podem ser em modo texto (linha de comando), por interface web, com um aplicativo específico do fabricante ou todas as opções. Em certos casos, um tipo de console de gerenciamento em linha de comando não possui todas as funcionalidades e é restrita para procedimentos simplificados, tais como a configuração de um endereço IP ou para salvar a configuração atual em um servidor remoto. Embora não exista uma padrão entre os fabricantes para a forma de aplicar os comandos, grande parte das funcionalidades disponíveis em switches são disponibilizadas por todos os fabricantes em seus equipamentos.

Neste livro serão apresentados os conceitos básicos das funcionalidades comuns em switches gerenciáveis, com exemplos de modelos de switches de gerações e fabricantes

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

diferentes. Espero que seja uma leitura proveitosa e que os procedimentos e conceitos disponibilizados contribuam na melhoria das rotinas de administração de redes. Boa leitura!

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

1) Conceitos Básicos

Neste capítulo serão apresentados os conceitos básicos sobre redes de computadores que são importantes para entender a operação dos switches.

1.1 Redes de Computadores

As redes de computadores tem como objetivo principal possibilitar a troca de dados, no formato de pacotes, entre aplicações remotas. Segundo o autor Tanenbaum, "*uma rede de computadores é um sistema de comunicação que interconecta dois ou mais dispositivos computacionais, permitindo a troca de dados e o compartilhamento de recursos*". Para que isto seja possível devem haver protocolos de suporte para que as aplicações troquem dados, sendo os principais protocolos os que fazem parte da família TCP/IP. Em redes locais, a comunicação direta entre os dispositivos utilizam o padrão IEEE 802.3, conhecido como padrão Ethernet, e suas variações. Além disso, são necessários dispositivos que façam a comunicação física e lógica das aplicações e sistemas operacionais que implementam os protocolos e as aplicações em rede. Para que a comunicação ocorra de forma universal foram definidos acordos e padrões para que fabricantes e desenvolvedores tornem compatível a comunicação entre os diversos tipos de equipamentos e aplicações.

Redes para Iniciantes - Como funciona uma rede? - https://youtu.be/5jf8HmFrs8s

Redes para Iniciantes - LAN, MAN, WAN... (Taxionomia de Redes) - https://youtu.be/sc-WkqfBN-c

1.2 Modelos de Referência OSI

O modelo de referência OSI (*Open Systems Interconnection*) é um modelo conceitual criado pela Organização Internacional de Normalização (ISO) que padroniza e descreve as funções de comunicação de um sistema de computação sem levar em consideração a estrutura interna e a tecnologia específica de cada sistema.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

O modelo OSI divide as funções de comunicação em sete camadas de abstração, cada uma com um conjunto específico de funcionalidades. Isso facilita a compreensão e a implementação de protocolos de rede, além de promover a interoperabilidade entre diferentes sistemas. Na Figura 1, está um diagrama que mostra a hierarquia das camadas.

Figura 1. Modelo de Referência OSI

As sete camadas do modelo OSI são:

- **Camada Física (*Physical Layer*)**:
    - Responsável pela transmissão de bits brutos através do meio físico, como cabos, fibras ópticas ou ondas de rádio
    - Define características elétricas, mecânicas e de temporização dos sinais
    - Exemplos de tecnologias: Ethernet, IEEE 802.11 (Wi-Fi), Bluetooth.
- **Camada de Enlace de Dados (*Data Link Layer*)**:

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

    - Responsável pela transmissão de quadros de dados entre dispositivos na mesma rede local
    - Controla o acesso ao meio físico e detecta erros de transmissão
    - Divide-se em duas subcamadas: MAC (*Media Access Control*) e LLC (*Logical Link Control*)
    - Exemplos de protocolos: Ethernet, PPP
- **Camada de Rede (*Network Layer*):**
    - Responsável pelo roteamento de pacotes de dados entre redes diferentes
    - Define o endereçamento lógico (endereços IP) e o roteamento de pacotes
    - Exemplos de protocolos: IP, ICMP
- **Camada de Transporte (*Transport Layer*):**
    - Responsável pela entrega confiável de dados entre aplicações em diferentes dispositivos
    - Controla o fluxo de dados e garante a integridade dos dados
    - Exemplos de protocolos: TCP, UDP
- **Camada de Sessão (*Session Layer*):**
    - Responsável pelo estabelecimento, gerenciamento e encerramento de conexões entre aplicações
    - Coordena a comunicação entre aplicações e sincroniza o diálogo
    - Exemplos de protocolos: NetBIOS, TLS
- **Camada de Apresentação (*Presentation Layer*):**
    - Responsável pela formatação e conversão de dados para garantir a compatibilidade entre aplicações
    - Realiza a criptografia e compressão de dados
    - Exemplos de formatos de dados: JPEG, ASCII
- **Camada de Aplicação (Application Layer):**
    - Responsável pela interface entre as aplicações e a rede
    - Fornece serviços de rede para as aplicações, como e-mail, navegação na web e transferência de arquivos
    - Exemplos de protocolos: HTTP, SMTP, FTP

O modelo OSI é uma ferramenta fundamental para entender como as redes de computadores funcionam e para desenvolver protocolos de comunicação eficientes e interoperáveis. Entretanto, por ser um modelo conceitual e que não foi adotado pelo mercado na íntegra, o modelo TCP/IP foi adaptado em camadas e é o padrão de fato para interconexão de dispositivos em rede.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

1.3 Modelo TCP/IP

O modelo TCP/IP (*Transmission Control Protocol/Internet Protocol)* é um conjunto de protocolos de comunicação que define como os dados são transmitidos pela Internet e outras redes de computadores. Foi desenvolvido na década de 1970 e se tornou o padrão para a internet na década de 1980, principalmente por estar implementado e disponível em sistemas Unix. O TCP/IP é fundamental para o funcionamento da Internet e é usado por praticamente todos os dispositivos conectados à rede. Este modelo foi adaptado de acordo com o modelo de referência OSI, com o agrupamento na camada de Aplicação das funcionalidades das camadas de Apresentação e Sessão no que resultou em um modelo em 5 camadas. Este modelo está demonstrado no diagrama da Figura 2.

Figura 2. Modelo TCP/IP em camadas

O modelo TCP/IP é organizado em quatro camadas (*RFC 1122 - Requirements for Internet Hosts -- Communication Layers*), adaptado para um modelo de 5 camadas de acordo com o modelo de referência OSI, cada uma com funções específicas. Na Camada de Aplicação são providos protocolos para serviços de rede tais como HTTP, HTTPS, SSH, SMTP, POP3 e centenas de outros protocolos que tratam diretamente dos dados gerados nas aplicações. Na Camada de Transporte devem estar os protocolos que realizam a entrega de

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

dados entre aplicações, por meio de protocolos como TCP e UDP. No protocolo UDP não há recursos de garantias de entrega controle de fluxo, funcionalidades disponíveis no protocolo TCP.

A Camada de Rede é responsável pelo roteamento de pacotes de dados entre redes diferentes. Nesta camada os protocolos principais são o IPv4, ICMP, IGMP, IPv6 e ICMPv6. Na Camada de Enlace estão as funcionalidades que controlam o acesso ao meio físico e transmitem dados entre dispositivos na mesma rede local. A Camada Física é a responsável por tratar da sinalização e dos meios físicos para que seja possível a comunicação entre os dispositivos em rede. O padrão Ethernet (IEEE 802.3) compreende as camadas de Enlace de dados e Física.

1.3 Pacotes

Um pacote de rede é a unidade básica de informação que trafega pela rede e é composto por uma parte de controle (cabeçalho ou *header*) e a área de dados (carga útil ou *payload*). Na parte do cabeçalho estão os parâmetros de controle que permitem o envio dos dados até o destino. Entre as informações contidas no cabeçalho estão os endereços de origem e destino dos pacotes. Estes endereços são distintos entre as camadas. Por exemplo, na camada de enlace de dados no padrão Ethernet, os endereços são conhecidos como MAC Address (Endereço Físico) e na camada de rede estão os endereços IPv4 e IPv6. Na Figura 3 um exemplo de um pacote capturado na ferramenta Wireshark do protocolo TCP com IPv4 em uma rede padrão Ethernet.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

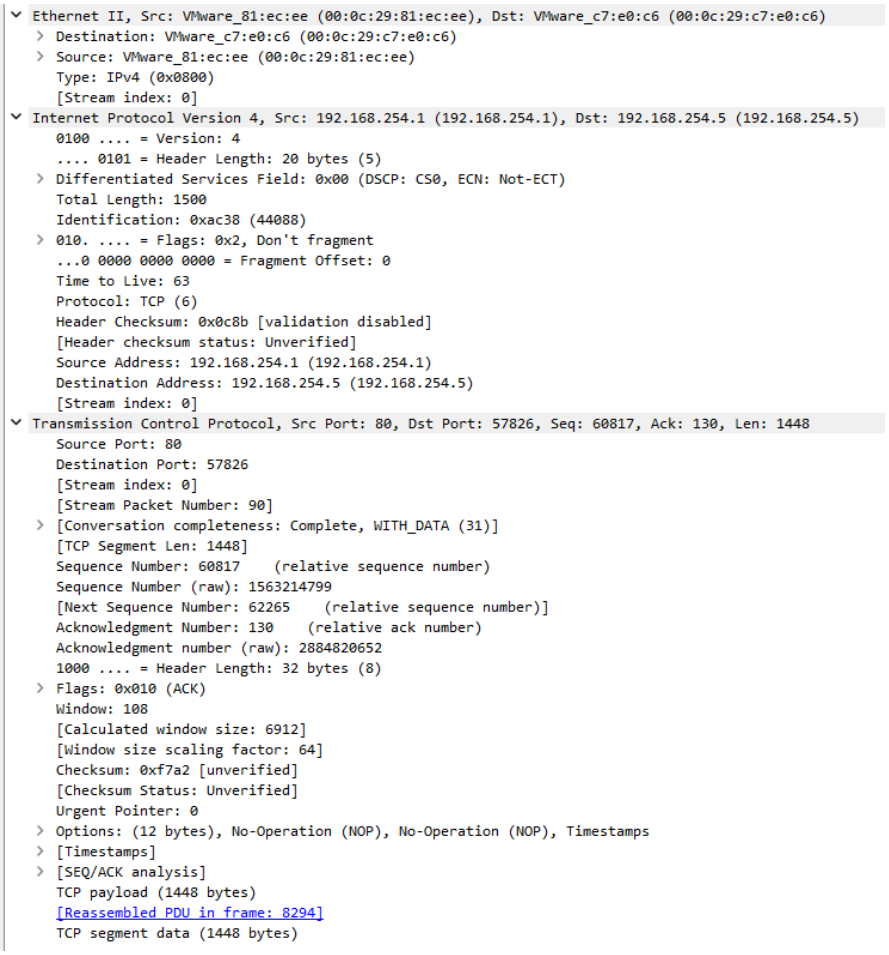


Figura 3. Pacote TCP capturado na ferramenta Wireshark

Os componentes de um pacote são:

- **Cabeçalho (*Header*):**
  - Contém informações de controle, como endereços de origem e destino (endereços IP e MAC), protocolos utilizados, parâmetros, opções, tamanho do pacote e outros dados para serem utilizados ao longo do caminho na rede entre origem e destino.
- **Dados (*Payload*):**
  - É a carga útil do pacote, ou seja, os dados reais que estão sendo transmitidos. Os dados são entregues aos processos no sistema operacional para serem utilizados de acordo com o serviço, por exemplo: texto, imagens e vídeos.
- **Rodapé (*Trailer*) ou Preâmbulo (SOF (*Start of Frame*)):**
  - Contém informações de verificação de erros, garantindo que o pacote não tenha sido corrompido durante a transmissão ou podem ser intervalos de bits

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

para manter a sincronia e detecção dos pacotes pelo destino ou dispositivos intermediários. O preâmbulo tem a função de anunciar a chegada de um pacote e tem como objetivo que a interface do receptor se prepare para o recebimento do pacote.

Redes para Iniciantes - Conceitos de Pacotes - https://youtu.be/7yH3LMwsOe0

1.4 Interface de Rede

As interfaces de rede Ethernet são o ponto de conexão físico entre um dispositivo (como um computador ou um switch) e o meio de transmissão da rede. Ao longo da história da Ethernet, essas interfaces evoluíram significativamente, acompanhando o desenvolvimento das tecnologias de cabeamento e as crescentes demandas por largura de banda.

Inicialmente, a Ethernet utilizava cabos coaxiais como meio de transmissão. As especificações 10BASE5 (Ethernet "*Thicknet*") e 10BASE2 (Ethernet "*Thinnet*") são exemplos dessa era. O 10BASE5, lançado em 1980, permitia velocidades de 10 Mbit/s e utilizava um cabo coaxial grosso que necessitava de transceivers externos para a conexão dos dispositivos. Sua instalação era complexa e cara. O 10BASE2, surgido em 1985, trouxe uma versão mais fina e flexível do cabo coaxial, facilitando a instalação, mas ainda compartilhando a limitação de um barramento comum onde todos os dispositivos dividiam a mesma largura de banda, tornando-o suscetível a colisões e falhas em caso de rompimento do cabo. Na Figura 4, um exemplo de uma rede com uso do padrão 10BASE2, sem uso de concentradores (hubs). A interface apresentada possui dois tipos de conexão para 10BASE2 e para 10BASET.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

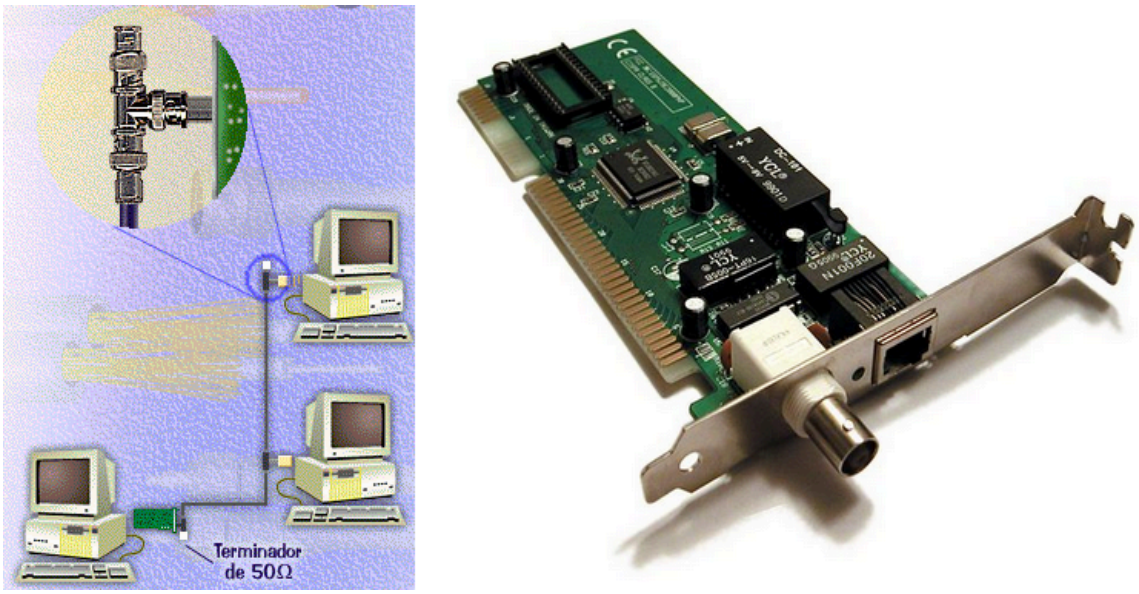


Figura 4. Conexões em 10BASE2

A grande virada veio com o advento do cabo de par trançado e as especificações 10BASE-T (1990) e 100BASE-TX (Fast Ethernet, 1995). O par trançado, especialmente o Categoria 5 (Cat5) e suas sucessores (Cat5e, Cat6, Cat6a, Cat7, Cat8), revolucionou a instalação de redes devido à sua flexibilidade, menor custo e facilidade de terminações com conectores RJ-45. A evolução continuou com as especificações 1000BASE-T (Gigabit Ethernet, 1999), 10GBASE-T (10 Gigabit Ethernet, 2006) e além, elevando as velocidades para 1 Gbit/s, 10 Gbit/s e, mais recentemente, 25 Gbit/s, 40 Gbit/s e 100 Gbit/s sobre par trançado de categorias mais elevadas, embora para as velocidades mais altas o alcance seja limitado. Na Figura 5, uma interface de rede com 4 conexões 1 Gbit/s.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

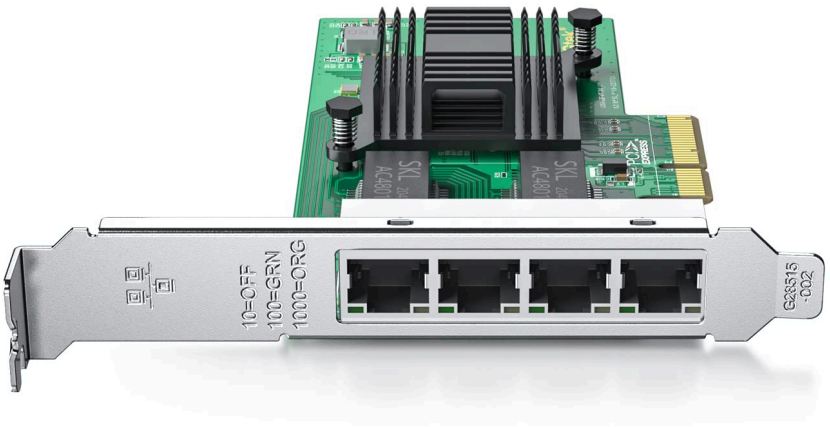


Figura 5. Interface de rede com 4 interfaces 1 Gbit/s

As interfaces de rede possuem funcionalidades e configurações que podem ser gerenciadas e são disponibilizadas pelo driver do fabricante. Na Figura 6, as opções de configuração de uma interface 1 Gbit/s em um sistema operacional Microsoft Windows 11.

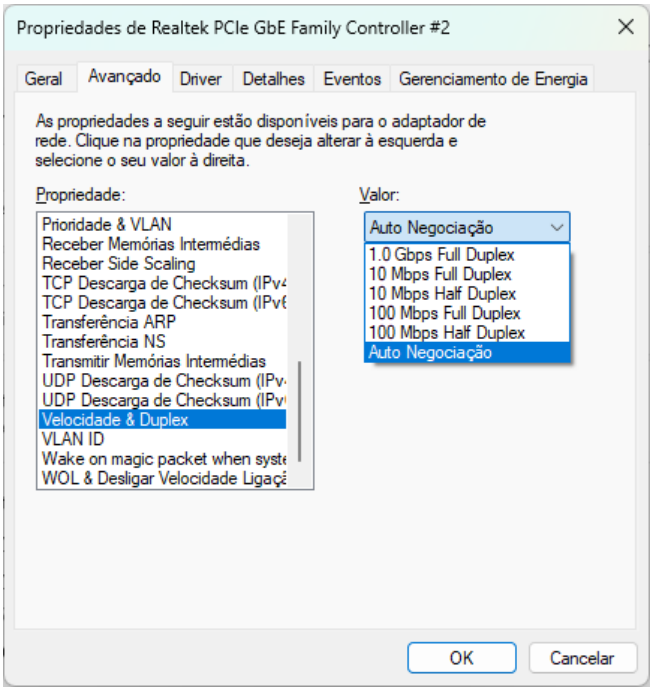


Figura 6. Opções de configuração em interfaces de rede (Microsoft Windows 11)

Em switches, mesmo os não gerenciáveis, as funcionalidades de Auto MDI/MDI-X e Auto Negociação são disponibilizadas por padrão. Por meio de detecção automática, a interface com o recurso de Auto MDI/MDI-X é capaz de identificar se o cabo de rede

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

conectado é um cabo reto (*straight-through*) ou um cabo cruzado (*crossover*). Uma vez detectado o tipo de cabo, a interface ajusta automaticamente a polaridade dos pinos de transmissão e recepção, garantindo que a comunicação ocorra corretamente, ou seja, pino de TX (transmissão) de um lado conectado ao pino de RX (recepção) do outro lado. Antes disto, o tipo de cabo a ser conectado em uma interface deveria ter conectorização diferente para poder funcionar. Em caso de uma conexão entre dois hubs, switches ou dois computadores, seria necessário um cabo *crossover* para que a transmissão de um lado fosse recebida pelo outro e vice-versa. Caso contrário, se o Auto MDI/MDI-X não estivesse disponível na interface, seria necessário um ajuste manual da ligação dos pares de fios dentro do cabo, o que seria inconveniente e propenso a erros.

Nos primeiros hubs e switches, essa limitação era contornada com a inclusão de portas especiais chamadas *uplink*. Essas portas tinham a polaridade de transmissão e recepção invertida internamente, permitindo o cascateamento (conexão entre hubs/switches) com um cabo reto, sem a necessidade de um cabo crossover. Em alguns casos, havia uma chave seletora para optar pelo uso da porta em modo normal ou em modo de *uplink*. No entanto, com a universalização do Auto MDI/MDI-X, a necessidade de portas *uplink* dedicadas praticamente desapareceu, tornando as conexões de rede mais simples. Na Figura 7, uma exemplo de porta de cascateamento em um hub e de uma chave seletora de modo operação da porta para normal ou para uso como *uplink*.

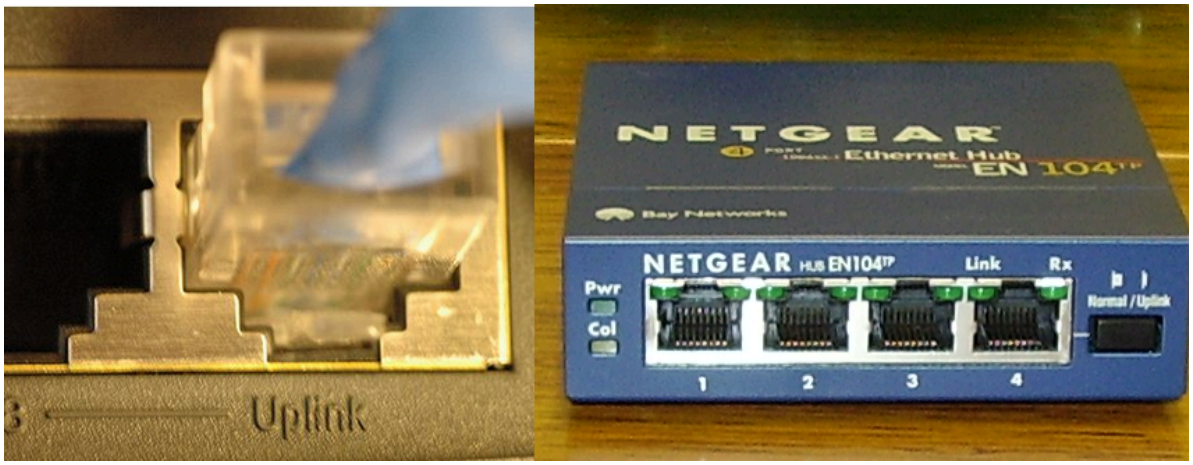


Figura 7. Interface de uplink em um hub

A Auto Negociação, também conhecida como NWay (um protocolo de auto negociação desenvolvido pela HP, popularmente associado ao conceito), opera na camada física do modelo OSI e permite que dois dispositivos conectados negociem e cheguem a um acordo sobre os melhores parâmetros operacionais comuns que ambos suportam. Ao estabelecer uma conexão, as interfaces de rede trocam informações sobre suas capacidades

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

utilizando *Normal Link Pulses* (NLPs), que são pulsos de sinal especiais> Um exemplo dos sinais NLP está Figura 8 que apresenta a troca de pulsos para a negociação de parâmetros. Através da análise desses pulsos, são negociados os parâmetros:

- Velocidade (*Speed*): Define a taxa de transferência de dados, tais como 10 Mbit/s, 100 Mbit/s, 1 Gbit/s e 10 Gbit/s
- Tipo de Transmissão (*Duplex Mode*): Decide se a comunicação será Half-Duplex (onde os dados são enviados e recebidos, mas não simultaneamente, exigindo que os dispositivos "se revezem") ou Full-Duplex (onde os dados podem ser enviados e recebidos ao mesmo tempo, maximizando o desempenho)
- Controle de Fluxo (*Flow Control*): Negocia a capacidade de pausar a transmissão de dados temporariamente para evitar que um emissor de pacotes exceda a capacidade de processamento de pacotes de um receptor, tipicamente usando quadros de pausa (*Pause Frames*)

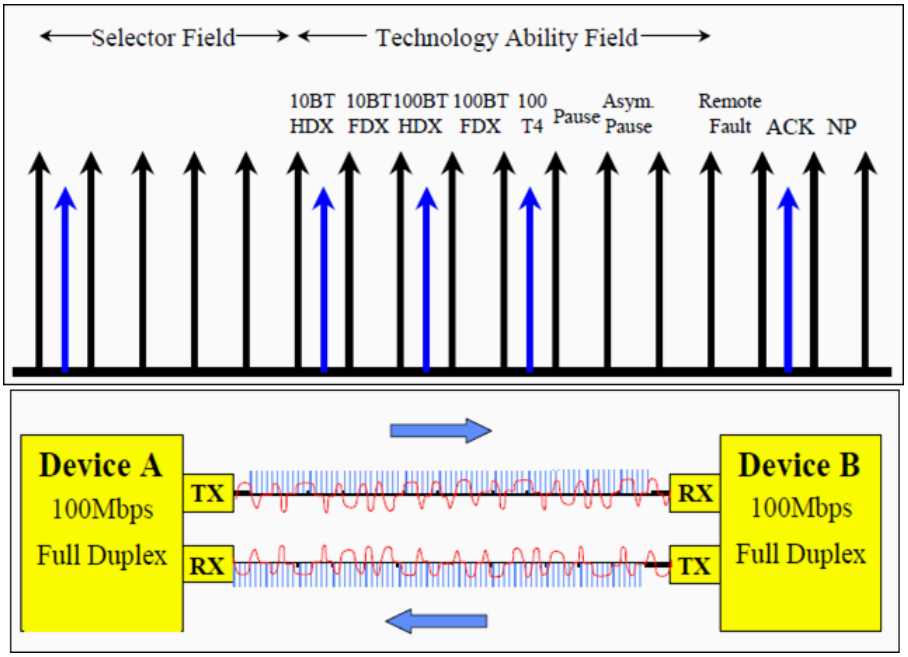


Figura 8. Negociação de parâmetros por meio de pulsos (NLPs)

A auto negociação segue uma hierarquia pré-definida para determinar o melhor parâmetro comum. As interfaces tentam negociar a configuração mais rápida e eficiente que ambas suportam. A ordem de preferência geralmente segue este padrão, do mais desejável ao menos desejável:

- 1000BASE-T Full Duplex (Gigabit Ethernet Full Duplex)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

- 1000BASE-T Half Duplex (Gigabit Ethernet Half Duplex - embora menos comum na prática para 1G, ainda é uma opção)
- 100BASE-T2 Full Duplex (Fast Ethernet sobre 2 pares, Full Duplex)
- 100BASE-TX Full Duplex (Fast Ethernet sobre 2 pares, Full Duplex)
- 100BASE-T2 Half Duplex (Fast Ethernet sobre 2 pares, Half Duplex)
- 100BASE-T4 (Fast Ethernet sobre 4 pares, Half Duplex)
- 100BASE-TX Half Duplex (Fast Ethernet sobre 2 pares, Half Duplex)
- 10BASE-T Full Duplex (Ethernet Padrão Full Duplex)
- 10BASE-T Half Duplex (Ethernet Padrão Half Duplex)

Apesar da sua eficiência, a auto negociação pode levar a problemas se houver uma configuração incorreta ou uma incompatibilidade entre os dispositivos. Um cenário não desejável que poderá acontecer com falhas na auto negociação é o *Duplex Mismatch* (incompatibilidade de modo duplex). Isso ocorre quando uma interface está configurada para *Full-Duplex* (seja manual ou por auto negociação correta), mas a outra interface está configurada para Half-Duplex (geralmente por configuração manual errada ou falha na auto negociação). Em um *Duplex Mismatch*, a interface *Half-Duplex* espera colisões e utiliza algoritmos para detectar sinal no meio físico antes de enviar pacotes (*listen before talk*), enquanto a interface *Full-Duplex* envia dados a qualquer momento, sem esperar. Isso resulta em um grande número de erros de colisão no lado *Half-Duplex* e perdas de pacotes no lado *Full-Duplex*, levando a uma degradação severa do desempenho da rede, mesmo em links com alta capacidade.

1.5 Endereço Fìsico (MAC Address)

Os endereços de origem e destino estão nos cabeçalhos dos pacotes e existem vários tipos e formatos de endereços, isto depende da função e camada de atuação e qual o tipo de comunicação a ser realizada, local ou remota. Em uma comunicação remota, onde os pacotes devem ser encaminhados por meio de roteamento, os endereços IPv4 ou IPv6 são utilizados para encontrar o destino final. Em uma comunicação local, por exemplo em rede do padrão Ethernet, onde os hosts estão conectados diretamente, serão usados endereços físicos (MAC Address) para a troca de dados.

Redes para Iniciantes - Endereçamento MAC - https://youtu.be/9ueE2e0Nzjs

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

O endereço MAC está relacionado com informações da interface de rede. O formato do endereço possui 6 Bytes, sendo dividido em 3 Bytes que identificam o fabricante, que funciona como um prefixo, e os outros 3 Bytes que identificam o número exclusivo da interface de rede, similar a um número de série. A funcionalidade deste tipo de endereço é a comunicação com dispositivos ligados na mesma rede de forma direta. O MAC Address é fixado pelo fabricante na interface de rede no processo de fabricação da placa. Na Figura 9 um exemplo de endereço MAC em uma interface de rede.

Figura 9. MAC Address em uma interface de rede padrão Ethernet

O nome MAC (*Medium Access Control*) vem da subcamada MAC na camada de enlace de dados. A alocação de endereços MAC é administrada pelo IEEE (https://standards.ieee.org/faqs/regauth/). O formato de representação é em hexadecimal (0-F) e a forma de apresentação de separadores do bytes poderá variar dependendo do fabricante, sendo as formas mais comuns de apresentação listadas na Tabela 1. Ainda existem alguns endereços MAC que possuem funcionalidades especiais, por exemplo FF:FF:FF:FF:FF:FF para indicar um destino em *broadcast* e 01:00:5E:XX:XX:XX que o prefixo indica um pacote em *multicast* e os últimos 3 Byes representam o grupo de multicast convertido do endereço IPv4 ou IPv6.

Tabela 1. Formatos de endereços MAC

Formato	**Exemplos de sistemas que utilizam o**

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

	formato
7c-8b-ca-75-7c-a0	Microsoft Windows **(este formato é o sugerido no padrão IEEE 802**)
7c:8b:ca:75:7c:a0	Linux
7c8b-ca75-7ca0	Switches HP
7c8b.ca75.7ca0	IOS (Cisco)

Random MAC Address -- https://youtu.be/DHlowrr6wc4

1.6 Dispositivos de Rede

Os dispositivos de rede fazem o encaminhamento dos pacotes entre origem e destino. São os responsáveis por serem os intermediários para dar suporte a comunicação remota entre aplicações e dispositivos finais. São dispositivos mais comuns de rede: switches, roteadores e APs (*Access Point*), *firewalls*, *hosts* e servidores.

Os switches são os dispositivos principais em uma rede local corporativa. Estes dispositivos operam na camada 2 (Enlace de Dados) do modelo OSI, aprendendo os endereços MAC dos dispositivos conectados às suas portas e encaminhando os quadros de dados apenas para a porta de destino correta. Devido a importância dos switches na rede, o gerenciamento destes dispositivos é uma das principais rotinas da administração de redes.

Os roteadores são dispositivos que atuam na camada 3 (Rede) do modelo OSI, sendo responsáveis por conectar diferentes redes (por exemplo, a rede local da empresa à Internet ou a outras filiais via VPNs). Eles tomam decisões de encaminhamento de pacotes com base nos endereços IP e nas tabelas de roteamento, escolhendo o melhor caminho para os dados alcançarem seus destinos. Em um ambiente corporativo, roteadores geralmente incluem funcionalidades de segurança como firewalls e VPNs.

Os *access points* (Pontos de Acesso) são os responsáveis por prover conectividade sem fio, realizando a conversão do tráfego de dados de dispositivos sem fio (notebooks,

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

smartphones, tablets) para a rede cabeada e vice-versa. Em ambientes corporativos, são comumente gerenciados centralizadamente por Controladores de APs, permitindo roaming transparente (trânsito do cliente entre APs destinos sem a perda de conexão), autenticação robusta (como 802.1X) e segmentação de rede via múltiplas SSIDs com diferentes VLANs.

Os *firewalls* são dispositivos de segurança que filtram o tráfego de rede com base em um conjunto de regras predefinidas, protegendo a rede corporativa contra acessos não autorizados e ataques. Podem ser baseados em hardware ou software e operam em diversas camadas do modelo OSI, inspecionando pacotes para permitir ou negar sua passagem. No caso de firewalls de próxima geração (NGFW) existem as funcionalidades de inspeção profunda de pacotes (DPI - *Deep Packet Inspection*), controle de aplicativos e prevenção de intrusões.

Os *hosts* são os dispositivos finais dos usuários onde as aplicações do lado cliente são executadas. Em uma rede local corporativa, esses hosts (como computadores, notebooks, smartphones e tablets) desempenham um papel central, permitindo que os colaboradores acessem recursos de rede, como servidores de arquivos, impressoras compartilhadas, bancos de dados e à Internet. Os *hosts* são os pontos de interação direta para a produtividade da empresa, sendo responsáveis por gerar e consumir o tráfego de dados que trafega pelos dispositivos intermediários.

Os servidores são o destino final ou a origem de grande parte do tráfego em uma rede local corporativa. Eles hospedam aplicativos, bancos de dados, serviços de arquivos, e-mail e diretórios (como *Microsoft Active Directory*), sendo fundamentais para as operações diárias da empresa e frequentemente conectados diretamente a switches de alta capacidade. Os sistemas operacionais instalados nos servidores implementam os protocolos de rede que propiciam a comunicação entre os dispositivos clientes (*hosts*) com os serviços disponibilizados pelos servidores.

Existem dezenas de fabricantes de dispositivos de rede e estes devem seguir os padrões e protocolos estabelecidos para haver compatibilidade entre os diversos tipos e modelos de equipamentos. Para garantir a interoperabilidade entre os equipamentos, os fabricantes devem seguir os padrões e protocolos estabelecidos por organizações de padronização tais como o IEEE e a IETF. Entretanto, devido a excelência e pioneirismo de alguns fabricantes, estes acabam se tornando o padrão do mercado e referência para os demais fabricantes. Um dos exemplos é a empresa Cisco. Esta empresa se tornou o padrão para dispositivos tais como roteadores, switches, *access points* e soluções de VoIP (Voz sobre IP). A forma de interação e o sistema operacional usado nos dispositivos da Cisco são referência na indústria há décadas e seu sistema operacional IOS *(Internetwork Operating*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

System) se tornou uma referência na configuração e gerenciamento de dispositivos de rede, principalmente em switches.

1.7 Ethernet (IEEE 802.3)

A rede Ethernet, padronizada como IEEE 802.3, é uma tecnologia de rede local (LAN) amplamente utilizada, que define as camadas física e de enlace de dados para comunicação em redes locais. A Ethernet é a base da maioria das redes locais e desempenha um papel fundamental na comunicação de dados em empresas, residências e *data centers*.

Desde sua primeira padronização em 1980, a Ethernet tem demonstrado uma capacidade notável de evolução. Essa constante adaptação às crescentes e diversas demandas das aplicações modernas foi o que a consolidou como o padrão principal em redes locais corporativas. Sua flexibilidade e escalabilidade permitiram que ela se mantivesse relevante, suportando desde o tráfego de dados mais simples até as complexas necessidades de largura de banda atuais, como vídeo em alta definição, virtualização e computação em nuvem.

Nos anos 70, a primeira rede experimental Ethernet foi implementada no computador Xerox Alto, permitindo que as estações de trabalho se comunicassem entre si e com servidores e impressoras a laser a uma taxa de transmissão de 2.94 Mbit/s. Um desenvolvimento fundamental nessa fase inicial foi o protocolo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) , que permite que os dispositivos "ouvissem antes de falar" e detectassem colisões, implementando um algoritmo de *backoff* para lidar com essas situações. Esta versão da Ethernet não foi usada comercialmente pela empresa Xerox, sendo posteriormente usada como base para o primeiro padrão IEEE 802.3.

Em 1980, a Digital Equipment Corporation (DEC), a Intel e a Xerox colaboraram para publicar uma especificação para Ethernet de 10 Mbit/s sobre cabo coaxial, que se tornou o padrão IEEE 802.3 em 1985. Essa padronização foi fundamental para a ampla adoção do Ethernet, que inicialmente competia com outras tecnologias de rede como a solução da IBM denominada Token Ring e diversas soluções proprietárias de redes locais. As primeiras implementações de Ethernet utilizavam mídia compartilhada, onde todos os dispositivos na rede compartilhavam o mesmo cabo para comunicação. Embora eficaz para redes pequenas com tráfego limitado, essa abordagem apresenta limitações significativas em termos de escalabilidade e eficiência. Na Figura 10, um exemplo de conexão em 10BASE5 com o uso de cabo coaxial como mídia e transceivers para conexão dos hosts na rede.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

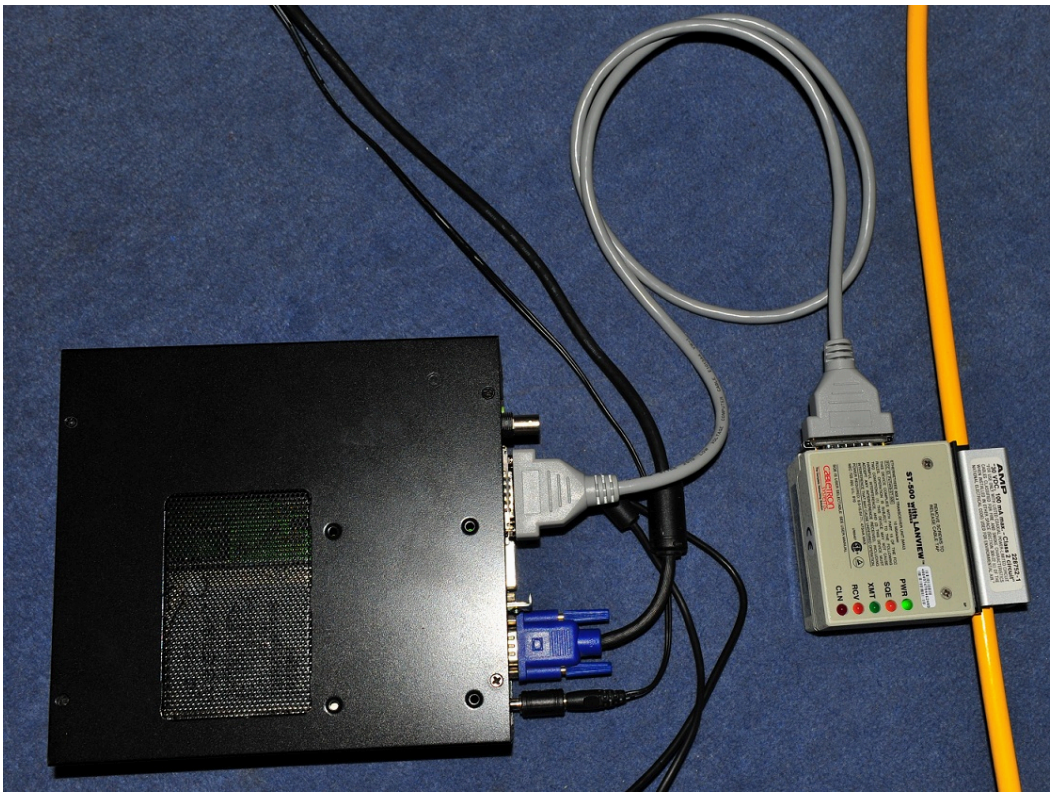


Figura 10. Conexões no padrão 10BASE5.

Na Tabela 2 uma breve linha do tempo com evolução das conexões em rede padrão Ethernet.

Tabela 2. Breve histórico da evolução das redes padrão Ethernet (IEEE 802.3)

Década	**Fatos**
1970	• Início: A Ethernet foi desenvolvida no Xerox PARC (*Palo Alto Research Center*) por Robert Metcalfe e seus colegas. A primeira versão experimental operava a 2,94 Mbit/s
1980	• 10BASE5 (1980): O primeiro padrão Ethernet comercial, usando cabo coaxial grosso (*thicknet*) e operando a 10 Mbit/s • 10BASE2 (1980s): Uma versão mais fina e flexível do cabo coaxial *(thinnet*), facilitando a instalação • IEEE 802.3 (1983): A Ethernet é padronizada pelo Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE)
1990	• 10BASE-T (1990): Introdução do cabo de par trançado, que se torna o padrão para redes locais • Fast Ethernet (100BASE-TX) (1995): Aumento significativo na velocidade, atingindo 100 Mbit/s

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

	• Gigabit Ethernet (1000BASE-T) (1999): Mais um salto de velocidade, chegando a 1 Gbit/s
2000	• 10 Gigabit Ethernet (10GbE) (2002): A Ethernet atinge velocidades de 10 Gbit/s, impulsionando a infraestrutura de data centers
2010	• 40 Gigabit Ethernet (40GbE) e 100 Gigabit Ethernet (100GbE): As velocidades continuam a aumentar para atender às demandas de *big data* e computação em nuvem • 25 Gigabit Ethernet (25GbE): Surgimento como uma opção de alta velocidade para *data centers*
2020	• 400 Gigabit Ethernet (400GbE) e além: A Ethernet continua a evoluir, com velocidades cada vez maiores para suportar aplicações como inteligência artificial e realidade virtual

À medida que mais dispositivos eram adicionados à rede, aumentava a probabilidade de colisões, levando à redução da taxa de transferência efetiva e à necessidade de mecanismos para gerenciar o acesso ao meio compartilhado. A largura de banda disponível era compartilhada entre todos os dispositivos, o que significava que o desempenho de cada dispositivo poderia ser afetado pelo tráfego gerado por outros. Essa limitação inerente da mídia compartilhada tornou evidente a necessidade de uma abordagem mais sofisticada para a criação de redes locais eficientes. As principais características das redes padrão Ethernet são:

- **Camada Física:**
  - Define as características elétricas e físicas dos cabos e conectores, bem como os métodos de sinalização para transmissão de dados
  - Suporta diversos tipos de mídia, incluindo cabos de par trançado e fibra óptica
- **Camada de Enlace de Dados:**
  - Define o formato dos quadros de dados e o protocolo de controle de acesso ao meio (MAC)
  - Utiliza endereços MAC para identificar dispositivos na rede
- **CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*):**
  - Método de acesso ao meio utilizado nas primeiras versões da Ethernet, que permitia que os dispositivos realizassem a detecção de colisões e tivessem a oportunidade de retransmissão dos dados
  - Em redes Ethernet modernas com switches, o CSMA/CD não é mais necessário devido ao funcionamento full-duplex
- **Switches:**

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

- Os switches Ethernet são dispositivos que encaminham o tráfego de dados com base nos endereços MAC, melhorando o desempenho da rede e reduzindo as colisões

- **Padrões IEEE 802.3:**
  - A família de padrões IEEE 802.3 define diversas variações da Ethernet, cada uma com diferentes velocidades, tipos de mídia e características
    - Exemplos são 10BASE-T, Fast Ethernet (100BASE-TX), Gigabit Ethernet (1000BASE-T) e 10 Gigabit Ethernet (10GBASE-T)

1.8 Cabeamento

O cabeamento é o principal meio físico de transmissão de qualquer rede local (LAN). Ao longo dos anos, a tecnologia de cabeamento evoluiu significativamente, acompanhando o aumento da demanda por largura de banda e velocidade. Uma breve evolução histórica do cabeamento utilizado em rede locais do padrão Ethernet:

- **Cabo Coaxial:**
  - Foi um dos primeiros tipos de cabeamento utilizados em redes
  - Consiste em um condutor central cercado por uma malha metálica e uma camada isolante
  - Embora robusto, era volumoso, caro e difícil de instalar
  - Foi amplamente utilizado nas primeiras redes Ethernet (10BASE5 e 10BASE2), mas gradualmente substituído pelo par trançado com o uso de hubs
- **Cabo de Par Trançado:**
  - Tornou-se o tipo de cabeamento mais comum em redes locais
  - Consiste em pares de fios de cobre trançados para reduzir a interferência eletromagnética
  - Existem diferentes categorias de cabos de par trançado, cada uma com diferentes especificações de desempenho
    - **Categoria 3 (Cat3):** Utilizado em telefonia e redes de baixa velocidade (10 Mbit/s)
    - **Categoria 5 (Cat5):** Suporta velocidades de até 100 Mbit/s
    - **Categoria 5e (Cat5e):** Versão aprimorada do Cat5, suportando velocidades de até 1 Gbit/s
    - **Categoria 6 (Cat6):** Suporta velocidades de até 10 Gbit/s em distâncias curtas
    - **Categoria 6A (Cat6A):** Suporta velocidades de até 10 Gbit/s em distâncias maiores
    - **Categoria 7 (Cat7) e 7A (Cat7A):** São cabos blindados, projetados para suportar frequências mais altas e velocidades de até 10 Gbit/s e 40 Gbit/s

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

        - **Categoria 8 (Cat8):** projetado para aplicações de data center, suporta velocidades de até 40 Gbit/s em distâncias curtas, e 25 Gbit/s em distâncias maiores
    - Existem dois tipos principais de cabos de par trançado:
        - **UTP (*Unshielded Twisted Pair*):** Não possui blindagem adicional
        - **STP (*Shielded Twisted Pair*):** Possui blindagem para proteção contra interferência
- **Fibra Óptica:**
    - Utiliza pulsos de luz para transmitir dados através de fibras de vidro ou plástico
    - Oferece alta largura de banda, baixa atenuação e imunidade a interferência eletromagnética
    - Ideal para longas distâncias e aplicações de alta velocidade, como *backbones* de rede e conexões de *data center*
    - Existem dois tipos principais:
        - Monomodo: ideal para longas distâncias
        - Multimodo: ideal para curtas distâncias

Redes para Iniciantes - Cabeamento - https://youtu.be/95j4N9-MJ2U

Redes para Iniciantes - Cabo UTP - https://youtu.be/5epJ4GjE8do

Redes para Iniciantes - Cabo de Fibra Ótica - https://youtu.be/CkWD2BUmckE

Cabeamento Categoria 7, 8 e padrão IEEE 802.3bz (NBASET) - https://youtu.be/ipDPj6KCKBI

1.9 Conectores

Em redes locais no padrão Ethernet (IEEE 802.3), os principais tipos de conectores utilizados para a conexão física dos dispositivos ao meio de transmissão são:

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **RJ45 (*Registered Jack* 45):** É o conector mais comum e amplamente utilizado para cabos de par trançado (UTP e STP). Possui oito pinos e é utilizado para conectar computadores, impressoras de rede, switches, roteadores, *access points* e outros dispositivos de rede às portas Ethernet dos equipamentos. Os cabos de par trançado com conectores RJ45 são a base da maioria das redes locais com fio, oferecendo diferentes categorias (Cat5e, Cat6, Cat6A, etc.) para suportar variadas velocidades de transmissão.

- **LC (*Lucent Connector*) e SC (*Subscriber Connector*):** São dois dos tipos mais comuns de conectores utilizados para cabos de fibra óptica.

    - **LC:** É um conector de pequeno formato com uma trava (latch), sendo popular em aplicações de alta densidade devido ao seu tamanho compacto. É frequentemente utilizado para conexões em switches, roteadores e outros equipamentos de rede que suportam interfaces de fibra óptica, especialmente para conexões Gigabit Ethernet (GBIC/SFP) e superiores.
    - **SC:** É um conector com um engate tipo *push-pull* (empurrar e puxar). Foi um dos primeiros conectores de fibra óptica padronizados e ainda é amplamente utilizado em diversas aplicações, incluindo conexões a switches, roteadores e outros equipamentos de rede com interfaces de fibra óptica.

- **GBIC (Gigabit Interface Converter) e SFP (*Small Form-factor Pluggable*)/SFP+ (*Enhanced Small Form-factor Pluggable*)/QSFP (*Quad Small Form-factor Pluggable*):** Embora não sejam conectores de cabo em si, são módulos transceptores que se encaixam em portas específicas de switches, roteadores e outros equipamentos de rede para fornecer interfaces de conexão para diferentes tipos de mídia (cobre ou fibra óptica) e diferentes velocidades. Eles possuem internamente os conectores apropriados para o tipo de cabo a ser utilizado (geralmente RJ45 para cobre e LC ou SC para fibra). A escolha do transceptor depende do tipo de cabo e da velocidade de conexão desejada.

- **Cabos DAC (Direct Attach Copper):** Diferente dos transceptores ópticos, que convertem sinais elétricos em luz, os cabos DAC utilizam a própria fiação de cobre para a transmissão de dados. Eles são passivos ou ativos (com eletrônica interna para amplificar o sinal em distâncias maiores) e vêm com conectores fixos, como SFP+, QSFP+, já acoplados em ambas as extremidades. Essa característica os torna ideais para ligações de curta distância, geralmente até 7 metros, dentro de racks ou entre

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

racks adjacentes, oferecendo alta largura de banda (10 Gbps, 25 Gbps, 40 Gbps, 100 Gbps e além) com baixa latência e custo reduzido em comparação com as soluções ópticas.

Fibra Ótica: Conversores - https://youtu.be/nAny7EUzjq8

Na Figura 11 um exemplo da instalação de conexões em um rack para um enlace de fibra óptica em uma rede padrão Ethernet.

Figura 11. Instalação de rede óptica em redes Ethernet

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Conexões com os Equipamentos:

- **Dispositivos Finais (Computadores, Impressoras, etc.):** Geralmente possuem uma porta Ethernet (RJ45) para conexão à rede através de um cabo de par trançado com conectores RJ45 nas duas extremidades (*patch cords*).

- **Switches e Roteadores:** Possuem múltiplas portas Ethernet (RJ45) para conectar os dispositivos finais e outros equipamentos de rede. Além disso, podem ter portas para módulos transceptores (GBIC, SFP, SFP+, QSFP) que permitem conexões de alta velocidade através de cabos de fibra óptica com conectores LC ou SC.

- **Access Points (APs):** Frequentemente possuem uma ou mais portas Ethernet (RJ45) para conexão à rede cabeada (geralmente a um switch ou roteador), permitindo que dispositivos sem fio se conectem à rede.

A maioria das conexões em redes locais Ethernet utiliza o conector RJ45 para cabos de par trançado, conectando dispositivos finais e equipamentos de rede. Para conexões de maior velocidade e/ou distâncias maiores, a fibra óptica com conectores LC ou SC, através de módulos transceptores (GBIC, SFP, etc.) inseridos em portas específicas dos equipamentos de rede, é a solução predominante. Na Figura 12 um exemplo de ponto lógico para conexão para um dispositivo do lado cliente.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

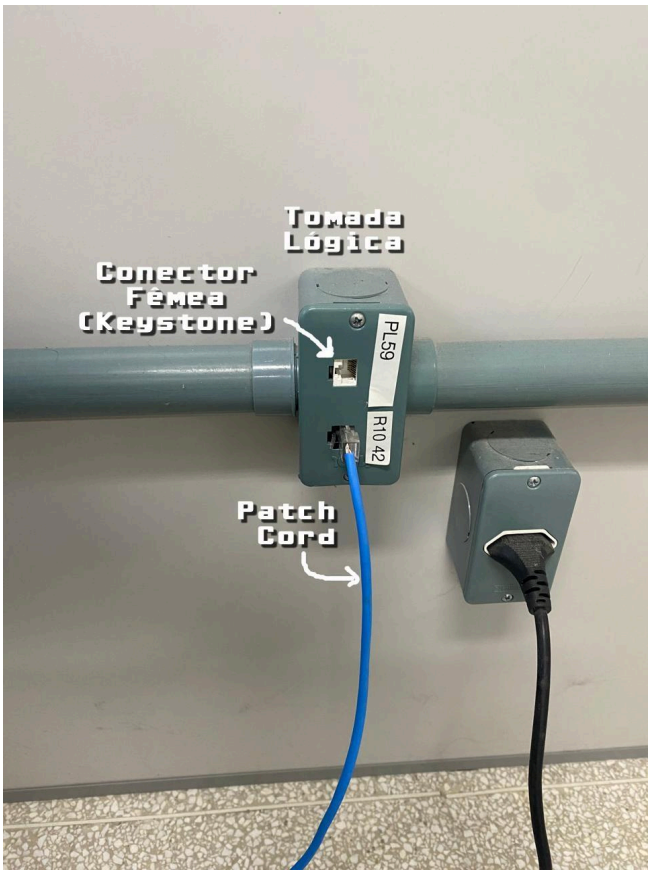


Figura 12. Ponto de rede lógico para conexão de dispositivo cliente.

1.10 Hubs

Os hubs são dispositivos de rede que operam na camada física (camada 1) do modelo OSI e funcionam como um ponto central de conexão para dispositivos em uma rede local (LAN). Sua função principal é receber sinais de um dispositivo e retransmiti-los para todos os outros dispositivos conectados, devido a este comportamento é denominado um hub repetidor. Ao contrário dos switches, que direcionam o tráfego com base nos endereços MAC, os hubs simplesmente replicam e enviam todos os dados recebidos para todas as portas. Isso significa que cada dispositivo na rede recebe todas as transmissões, independentemente de ser o destinatário pretendido.

Como todos os dispositivos compartilham o mesmo meio de transmissão, colisões de dados podem ocorrer quando dois ou mais dispositivos tentam transmitir simultaneamente. Isso pode resultar em perda de dados e diminuição do desempenho da rede. A topologia física de um hub é em estrela, entretanto, a topologia lógica é em barramento onde todos os

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

hosts disputam um meio físico compartilhado para poderem transmitir. O controle é feito pelo algoritmo CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) que é executado em cada interface de rede dos hosts conectados ao hub.

Como principais características dos hubs está a simplicidade. Os hubs são dispositivos simples, com pouca ou nenhuma capacidade de processamento ou configuração e possuem custo baixo sendo mais baratos que os switches. Devido à sua natureza de transmissão indiscriminada, os hubs podem levar a congestionamento de rede e baixa eficiência, especialmente em redes com grande tráfego de dados. Na Figura 13, um exemplo de hub no padrão 10BASET.

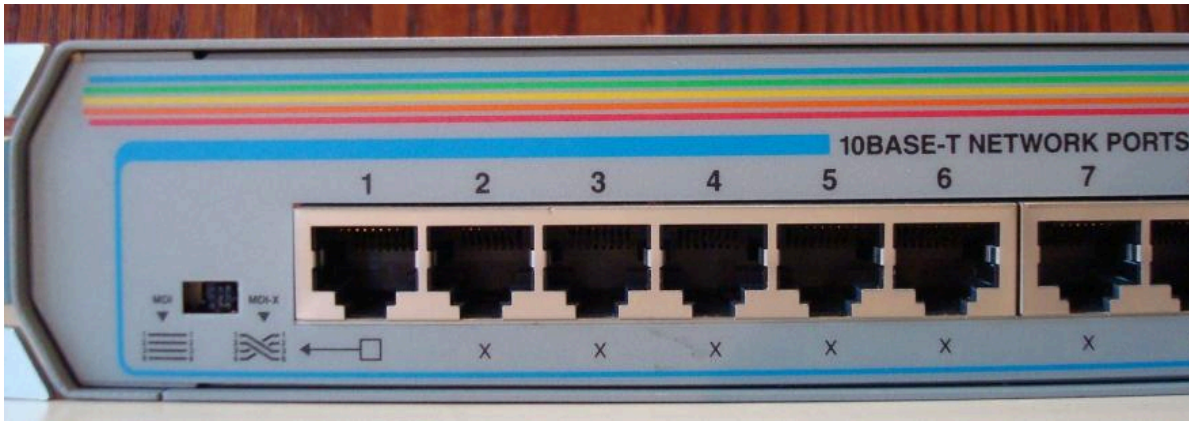


Figura 13. Exemplo de hub compatível com o padrão 10BASET.

Os hubs foram amplamente utilizados em redes Ethernet mais antigas, mas foram gradualmente substituídos por switches. Os switches oferecem desempenho superior, pois direcionam o tráfego de forma inteligente, reduzindo as colisões e melhorando a eficiência da rede. Atualmente os hubs são considerados obsoletos, e seu uso é muito raro e não há mais este dispositivo à venda no mercado.

Ainda existem hubs? - https://youtu.be/9KuHBdotRNI

Cascateamento de Hubs - https://youtu.be/1MJHEJNOljk

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

1.11 Bridges

As bridges, ou pontes de rede, são dispositivos que operam na camada 2 (enlace de dados) do modelo OSI e têm como função principal conectar segmentos de rede local, permitindo que se comuniquem como se fossem uma única rede. Estes dispositivos foram uma evolução em relação aos hubs e tiveram papel importante no surgimento dos switches. As bridges analisam os endereços MAC (*Media Access Control*) dos pacotes. Com base nesses endereços, elas determinam se um pacote deve ser encaminhado para outro segmento da rede ou se deve ser mantido no segmento atual. Essa análise e encaminhamento seletivo ajudam a reduzir o tráfego desnecessário na rede, otimizando o desempenho.

As principais funções e características das bridges são

- **Segmentação de rede**
  - Dividem uma LAN grande em segmentos menores, o que reduz o domínio de colisão e melhora a eficiência da rede.
- **Filtragem de tráfego**
  - Ao analisar os endereços MAC, as bridges evitam que pacotes desnecessários sejam transmitidos para todos os segmentos, diminuindo o congestionamento.
- **Conexão de segmentos diferentes**
  - Podem conectar segmentos de rede que utilizam diferentes meios físicos. Nos primórdios das redes locais, onde haviam padrões distintos como Ethernet e Token Ring, as bridges possibilitaram a tradução dos pacotes para prover a comunicação entre estas redes. Um exemplo atual é o uso de *access points* operando como *bridges*, tornando possível a troca de pacotes de forma transparente entre hosts na rede cabeada e na rede sem fios.
- **Aprendizagem de endereços MAC**
  - As bridges mantêm uma tabela de endereços MAC, aprendendo quais dispositivos estão conectados a cada segmento da rede.

As *bridges* foram um passo importante na evolução das redes, representando uma melhoria em relação aos hubs, que simplesmente retransmitem todo o tráfego. Com o avanço da tecnologia, os switches de camada 2 passaram a desempenhar as funções das *bridges*, oferecendo recursos mais avançados e maior desempenho.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

1.12 Switches

Os switches Ethernet são dispositivos de rede essenciais que conectam vários dispositivos em uma rede local, facilitando a comunicação eficiente entre eles. Na década de 1990, os switches Ethernet emergiram como a solução definitiva para a conectividade em LANs. Similar às *bridges* e ao contrário dos hubs, que transmitem dados para todos os dispositivos conectados, os switches analisam os endereços MAC (*Media Access Control*) dos pacotes de dados e os encaminham apenas para o dispositivo de destino pretendido. Isso reduz o tráfego desnecessário na rede e melhora o desempenho. Os switches mantêm uma tabela de endereços MAC, que mapeia os endereços MAC dos dispositivos conectados às suas respectivas portas. Essa tabela permite que os switches determinem a porta de saída correta para cada pacote de dados. As principais características dos switches são:

- **Camada 2 do Modelo OSI**
  - Os switches operam na camada de enlace de dados, responsável pela transmissão de quadros de dados entre dispositivos na mesma LAN.
- **Múltiplas Portas**
  - Os switches possuem várias portas para conectar dispositivos, com portas metálicas, para conexões de fibra ou uso de módulos SFP. A quantidade de portas em switches varia de 2 até centenas de portas em configurações com empilhamento ou em dispositivos modulares.
- **Velocidade e Desempenho**
  - Os switches oferecem alta velocidade de transmissão de dados e melhoram o desempenho da rede em comparação com os hubs. As velocidades variam de 10 Mbit/s até 100 Gbit/s e estão em constante evolução.
- **Tipos de Switches**
  - **Não gerenciáveis**
    - São dispositivos *plug-and-play* simples, sem opções de configuração avançadas.
  - **Gerenciáveis**
    - Oferecem recursos avançados de configuração, como VLANs (*Virtual LAN*), monitoramento, QoS (qualidade de serviço) e segurança.

A denominação não-gerenciável ou gerenciável é determinada pelas funcionalidades do switch. Uma das principais motivações para adoção do padrão Ethernet em redes corporativas foi a centralização das conexões em hubs, posteriormente em switches. Desta forma, tornou-se possível gerenciar a rede por meio de um único dispositivo. No início da evolução dos switches, a distinção entre um modelo gerenciável e um não-gerenciável era bem mais simples. Basicamente, um switch era considerado gerenciável se permitisse o monitoramento do tráfego nas suas portas e oferecesse um acesso remoto para visualizar estatísticas – muitas vezes, isso era feito por meio console serial ou com emulação de

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

terminal via protocolo Telnet. Essencialmente, um switch não-gerenciável era o mesmo hardware, mas sem esse módulo básico que permitia a interação e o controle mínimos. Essa funcionalidade inicial, apesar de rudimentar pelos padrões atuais, já fornecia aos administradores de rede uma visibilidade fundamental sobre o que acontecia na infraestrutura.

Com a evolução dos padrões e protocolos de gerenciamento, principalmente do protocolo SNMP (*Simple Network Management Protocol*), e de novas funcionalidades adicionadas pelos fabricantes, sendo algumas proprietárias, o conceito de um switch gerenciável mudou consideravelmente. Atualmente, mesmo um switch não-gerenciável possui algumas funcionalidades avançadas que são aplicadas automaticamente, por exemplo múltiplas filas de QoS e PoE (Power over Ethernet). A principal diferença entre um switch gerenciável e um não gerenciável reside, de fato, na capacidade de configurar e personalizar suas funcionalidades. Enquanto um switch não gerenciável opera com configurações predefinidas de fábrica, um switch gerenciável oferece ao administrador de rede o controle total para ajustar, monitorar e otimizar o comportamento do dispositivo e, consequentemente, da rede.

Na Tabela 3, uma comparação resumida das características entre dois switches do mesmo fabricante, sendo um não-gerenciável e o outro gerenciável.

Tabela 3. Características de switches não-gerenciáveis e gerenciáveis

Switch não-gerenciável	**Switch gerenciável**
24 portas, 10/100/1000 Mbit/s, 256KB SRAM, Backplane (Capacidade de comutação) 48 Gbit/s, Taxa de encaminhamento de pacotes 35,71 Mpps, Latência 3,127 us, Configuração de portas Autonegociação, MDI/MDI-X Protocolo CSMA/CD. QoS Algoritmo de enfileiramento WRR (Weighted Round Robin)	*24 portas 10/100/1000, 4 portas SFP+ 1/10Gbits, Porta console, Memória 512 MB, Memória flash 256 MB, dual boot image, Backplane (Capacidade de comutação) 128 Gbit/s, Taxa de encaminhamento de pacotes 95.232 Mpps, Latência 2.600 µs, VLANs, Espelhamento de Portas, Autonegociação, MDI/MDI-X, Agregação de Portas, Spanning-Tree, QoS, Segurança em Portas, Acesso remoto por linha de comando e interface web, ACL, DHCP Snooping, SNMP, sFLOW, LLDP, Loop Protection, Layer 3*

Hubs e Switches - https://youtu.be/BQvlv0ktGfs

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

1.13 Switches Gerenciáveis

A evolução das funcionalidades em switches gerenciáveis tem sido impulsionada pela crescente complexidade das redes e pela demanda por maior controle, segurança e desempenho. Na Tabela 4 está um breve histórico da evolução das funcionalidades em switches gerenciáveis.

Tabela 4. Histórico da Evolução das Funcionalidades em Switches Gerenciáveis

Evento	Funcionalidades
Gerenciamento Básico (Década de 1990)	• **Configuração via CLI (Interface de Linha de Comando):** Os primeiros switches gerenciáveis ofereciam configuração básica por meio de comandos de texto. • **SNMP (*Simple Network Management Protocol*):** Permitir o monitoramento básico do tráfego e do status do switch. • **VLANs (Redes Locais Virtuais):** A capacidade de segmentar a rede em VLANs para melhorar a segurança e o desempenho.
Recursos Avançados de Camada 2 (Década de 2000)	• **QoS (Qualidade de Serviço):** A priorização do tráfego tornou-se essencial para aplicações sensíveis à latência, como VoIP e vídeo. • **STP (*Spanning Tree Protocol*):** Evitar loops de rede, garantindo a estabilidade da rede. • **Agregação de Links (Link Aggregation):** Aumentar a largura de banda e a redundância da rede. • **Segurança de Porta:** Recursos como *Port Security* e IEEE 802.1X para controlar o acesso à rede.
Funcionalidades de Camada 3 e Roteamento (Década de 2010)	• **Roteamento Estático e Dinâmico:** Alguns switches gerenciáveis começaram a oferecer recursos de roteamento de Camada 3, permitindo a comunicação entre VLANs e redes diferentes.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

	• **Listas de Controle de Acesso (ACLs):** Fornecer controle granular sobre o tráfego de rede, melhorando a segurança. • **PoE (Power over Ethernet):** A capacidade de fornecer energia aos dispositivos conectados para simplificar a implantação de telefones IP, câmeras de segurança e pontos de acesso sem fios.
Automação e SDN (Redes Definidas por Software) (Década de 2020)	• **APIs (Interfaces de Programação de Aplicativos):** Permitir a automação e a integração com outras ferramentas de gerenciamento de rede. • **SDN (Redes Definidas por Software):** Separar o plano de controle do plano de dados, permitindo o gerenciamento centralizado e a programação da rede. • **Análise de Tráfego:** Recursos avançados de análise de tráfego fornecem informações detalhadas sobre o desempenho da rede e possíveis problemas. • **Segurança Aprimorada:** Detecção de ameaças e respostas automatizadas para combater ataques.

Nos anos 90, algumas empresas como 3Com e Cisco ofereciam hubs com capacidade de gerenciamento por linha de comando e console web. As funcionalidades eram bem simplificadas, mas já era possível monitorar o tráfego das portas ou realizar ações como bloquear portas. Com a evolução para os switches houve um momento de transição, onde as empresas necessitam migrar de tecnologia compartilhada para a tecnologia comutada provida por switches. Entretanto, o alto custo dos switches era um impedimento para a maioria das redes locais de pequeno e médio porte. Um switch gerenciável com poucas portas Fast Ethernet (100 Mbit/s) poderia custar milhares de dólares, refletindo a natureza inovadora da tecnologia e a produção em menor escala. As funcionalidades de gerenciamento ainda eram bem limitadas, mesmo em switches usados no *core* (núcleo) da rede.

Com o surgimento de inúmeros fabricantes de switches, de gigantes como Cisco e HPE a empresas focadas em redes de menor porte e residenciais tais como TP-Link, Ubiquiti e D-Link, intensificou a concorrência no mercado. Para conquistar fatia de mercado, as empresas foram obrigadas a inovar e reduzir seus custos. Os fabricantes passaram a oferecer diferentes níveis de switches gerenciáveis.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

Enquanto os modelos de grande porte para uso em *data centers* e no *core* de redes em grandes empresas continuam com alto custo devido às suas funcionalidades avançadas e desempenho extremo, surgiram categorias como *smart switches* ou *web-managed switches* que oferecem um subconjunto de recursos gerenciáveis a um custo muito mais baixo, atendendo às necessidades de redes menores com uma necessidade de investimento dentro da realidade das pequenas e médias empresas.

Nos anos 2000 a empresa Cisco publicou uma forma de categorizar os tipos de switches gerenciáveis de acordo com a aplicação dentro da arquitetura da rede. Desta forma, estabeleceu um modelo hierárquico, dividindo a infraestrutura em três camadas principais: acesso, distribuição e *core* (núcleo). Essa segmentação não só organiza a rede de forma lógica, mas também influencia diretamente o tipo de switch necessário em cada camada de acordo com as funcionalidades e, consequentemente, com o custo do dispositivo.

Na Tabela 5 uma breve descrição do modelo hierárquico de 3 camadas da empresa Cisco. Embora as ideias de segmentação e hierarquia em redes já circulassem de maneira menos estruturada, a formalização desse modelo representou um marco. Ele foi fundamental para estabelecer como uma melhor prática da indústria o projeto de redes corporativas. Devido a essa abordagem, tornou-se possível criar infraestruturas que não apenas são escaláveis para acompanhar o crescimento das empresas, mas também confiáveis para suportar operações críticas e eficientes na entrega de dados e serviços.

Tabela 5. Modelo hierárquico de 3 camadas da empresa Cisco

Camada	**Descrição**
Acesso	É a porta de entrada da rede para os dispositivos finais (computadores, impressoras, telefones IP, câmeras de segurança). Nesses equipamentos, funcionalidades como *Power over Ethernet* (PoE/PoE+) para alimentação de dispositivos, segurança de porta (*Port Security*), VLANs para segmentação de tráfego e Qualidade de Serviço (QoS) básica para priorização de aplicações (como voz e vídeo) são essenciais. O custo por porta é um fator crítico, e a demanda por alta densidade de portas é comum.
Distribuição	Atuam como um ponto intermediário, agregando o tráfego de vários switches de acesso e fornecendo conectividade de camada 3 (roteamento) para as VLANs. Aqui, a capacidade de encaminhamento, a redundância (fontes de alimentação duplas, módulos de controle) e funcionalidades de camada 3 (roteamento inter-VLAN, OSPF, EIGRP) são comuns. Eles também implementam políticas de segurança mais robustas e atuam como pontos de agregação para *uplinks* de alta velocidade. O custo é significativamente maior que o dos switches de acesso, refletindo sua maior complexidade e desempenho.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Core (Núcleo)	Representam o *backbone* da rede, sendo responsáveis por encaminhar o tráfego em alta velocidade entre os switches de distribuição e para a Internet/outras redes externas. Esses switches são o ponto mais crítico da rede e exigem o máximo em desempenho (velocidades de 10Gbit/s, 40Gbit/s, 100Gbit/s ou mais), redundância extrema, escalabilidade (chassis modular, alta densidade de portas) e funcionalidades avançadas de roteamento (BGP). O custo desses equipamentos é o mais elevado, justificando-se pela necessidade de garantir a menor latência e a maior disponibilidade para toda a rede.

Uma das principais diferenças entre switches não gerenciáveis e gerenciáveis está na necessidade de realizar configurações para tornar o switch operacional. Em switches não gerenciáveis basta ligar o equipamento que em poucos segundos estará funcional, bastando conectar fisicamente os cabos. Em um switch gerenciável o tempo de inicialização do sistema operacional poderá levar vários minutos até o dispositivo ficar operacional. Na Tabela 6, os tempos de inicialização aproximados para switches gerenciáveis de vários níveis de capacidade.

Tabela 6. Tempos de inicialização para switches de vários níveis de capacidade.

Tipo de Switch / Cenário	**Tempo de Inicialização (Até Operacional)**	**Fatores que Influenciam e Observações**
Switches de Borda/Acesso (modelos de entrada)	1 a 3 minutos	Geralmente possuem menos recursos e um sistema operacional mais leve. Ideal para escritórios menores e redes de acesso.
Switches de Distribuição/Agregação (modelos intermediários)	3 a 7 minutos	Mais recursos, maior capacidade de processamento e um sistema operacional mais completo. Comuns em redes maiores, conectando várias VLANs.
Switches de Core (modelos avançados/enterprise)	5 a 15 minutos (ou mais)	Alta performance e grande porte, com sistemas operacionais robustos e módulos adicionais. Essenciais para backbones de grandes redes e data centers.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Qualquer Switch Gerenciável (primeira inicialização ou grandes atualizações)	Pode levar 10-20 minutos ou mais	Na primeira vez que é ligado ou após atualizações de firmware significativas, o switch pode precisar de tempo extra para descompactar arquivos, aplicar configurações padrão ou migrar dados, além de realizar um ou mais reboots.

Além disso, em muitos casos, as portas podem estar desabilitadas de forma administrativa, que demanda um acesso inicial por meio da console de gerenciamento para ativação das portas. Apesar dessa curva de aprendizado inicial, as vantagens do uso de switches gerenciáveis na administração de redes são inquestionáveis. Eles oferecem um controle sobre o desempenho e a segurança da rede, permitindo otimizações que simplesmente não são possíveis com switches não gerenciáveis. Essa capacidade de gerenciamento e personalização é essencial para redes corporativas e ambientes que demandam alta performance e confiabilidade.

O investimento em switches gerenciáveis é uma opção estratégica em qualquer empresa. Enquanto o custo inicial de um switch gerenciável pode ser superior ao de um switch não gerenciável, os benefícios a longo prazo em termos de segurança, desempenho, confiabilidade e facilidade de gerenciamento superam amplamente o investimento. Os switches gerenciáveis são os principais dispositivos de uma infraestrutura de rede corporativa.

Switches Gerenciáveis - https://youtu.be/37pqbjy2C6I

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

2) Instalação Física

Os procedimentos corretos para a instalação física de switches são essenciais para garantir a operação eficiente, a confiabilidade e a longevidade da infraestrutura de rede de uma organização. Uma instalação inadequada pode resultar em problemas de desempenho, falhas de hardware inesperadas e dificuldades significativas na manutenção e solução de problemas futuros. Este capítulo aborda os principais aspectos a serem considerados durante a instalação física de switches, incluindo a escolha da localização, os requisitos de ventilação, as conexões de energia, os métodos de acesso à interface de console, as credenciais de autenticação padrão, a instalação em racks e os procedimentos para restaurar as configurações de fábrica.

2.1 Acesso a Porta de Console

O acesso à porta de console de um switch é essencial para a configuração inicial, solução de problemas e recuperação do dispositivo. Existem principalmente duas formas de acesso local por conexão serial (RS-232) e por conexão via USB:

Conexão Serial (RS-232): A maioria dos switches possui uma porta de console, geralmente com um conector RJ-45 ou DB-9, que permite o acesso direto à interface de linha de comando (CLI). Para estabelecer uma conexão serial, é necessário um cabo de console apropriado. Para portas RJ-45, geralmente é utilizado um cabo *rollover* RJ-45 para DB-9.

Para computadores que não possuem porta serial DB-9, um adaptador USB para serial pode ser utilizado em conjunto com o cabo de console. No computador, é preciso configurar um software de emulação de terminal, como PuTTY ou Tera Term, com os parâmetros corretos para uso da porta serial. Os parâmetros típicos incluem a velocidade de transmissão (*baud rate*), que geralmente é 9600 bit/s, 8 bits de dados, 1 bit de parada, paridade nenhuma e controle de fluxo nenhum.

Após conectar o cabo e configurar o software, ao ligar o switch, o prompt de comando deve aparecer na tela do terminal, permitindo a interação com o dispositivo. A conexão serial é o método mais comum para o acesso inicial, especialmente quando o acesso à rede ainda não foi configurado ou em situações de recuperação de falhas.

Conexão via USB: Alguns modelos de switches oferecem uma porta de console USB, geralmente com um conector mini-USB ou USB-C, como uma alternativa à porta serial tradicional. Para utilizar essa conexão, é necessário um cabo USB adequado, como um cabo USB-A para mini-USB ou USB-A para USB-C. Em muitos casos, pode ser necessário instalar drivers específicos fornecidos pelo fabricante do switch no sistema operacional do computador para que a porta USB seja reconhecida como uma porta serial virtual.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Após a instalação dos drivers, a configuração do software de emulação de terminal é semelhante à da conexão serial, mas é preciso selecionar a porta COM correspondente à interface USB serial virtual no gerenciador de dispositivos do computador. A conexão USB oferece uma alternativa mais conveniente para computadores modernos que não possuem portas seriais nativas, mas a necessidade de instalação de drivers pode ser um fator a considerar.

Na Figura 14, a conexão na console usando a porta serial em um switch Huawei modelo S5735-L24P4S-A1.

Figura 14. Conexão na porta console em um switch Huawei S5735-L24P4S-A1.

2.2 Conexão Serial

Para que o computador consiga se comunicar com o switch através da conexão serial estabelecida pelo cabo *rollover*, é necessário configurar um software de terminal com os parâmetros corretos. Os principais parâmetros de conexão serial são:

- ***Baud Rate* (Velocidade):** Define a taxa de transferência de dados em bits por segundo. É necessário que essa configuração corresponda à velocidade configurada na porta de console do switch. As velocidades mais comuns são 9600, 19200 e 38400 bit/s.
- ***Data Bits* (Bits de Dados):** Especifica o número de bits utilizados para representar cada caractere transmitido. O valor mais comum é 8.
- ***Parity* (Paridade):** É um método simples de verificação de erros na transmissão de dados. A configuração mais comum é *None* (Nenhum).
- ***Stop Bits* (Bits de Parada):** Sinaliza o final de um caractere transmitido. O valor mais comum é 1.
- ***Flow Control* (Controle de Fluxo):** Mecanismo para gerenciar a taxa de transmissão de dados entre o computador e o switch, evitando a perda de dados. A configuração mais

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

comum é *None* (Nenhum).

Na Figura 15, um exemplo de configuração para acesso a porta serial utilizando a ferramenta Putty em um sistema operacional Microsoft Windows 11.

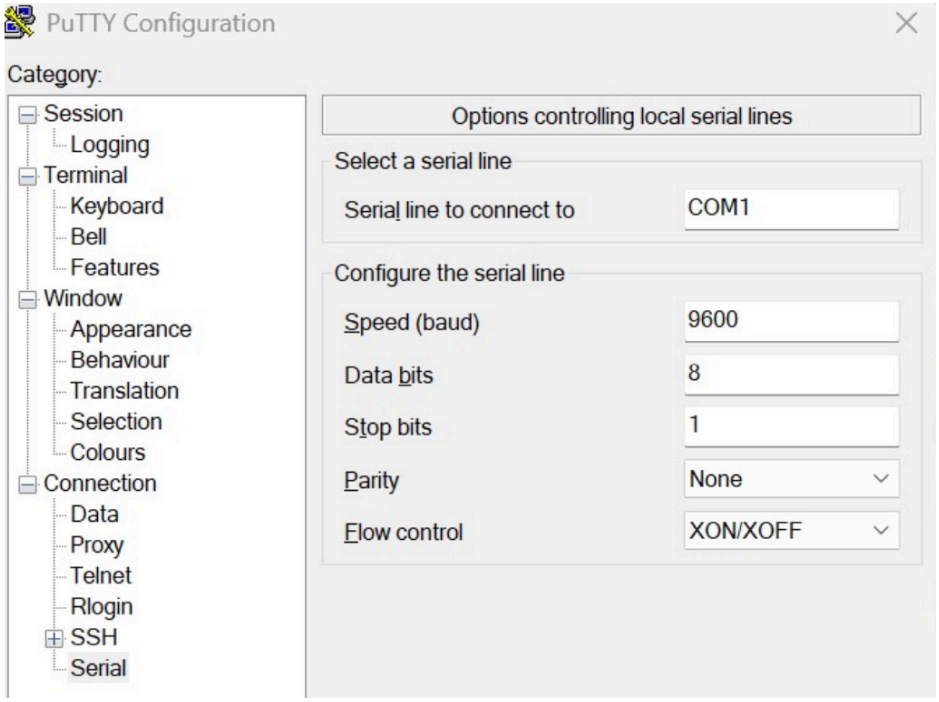


Figura 15. Configuração de acesso a porta serial com a ferramenta Putty.

Os parâmetros corretos estão disponíveis na documentação do equipamento ou gravado no próprio equipamento, geralmente próximo a porta de console. O uso de configurações incorretas no software de emulação de terminal é uma das causas mais comuns de falha ao tentar acessar a console de um switch. Embora as configurações exatas possam variar dependendo do fabricante e do modelo do switch, algumas configurações padrão são frequentemente utilizadas:

- ***Baud Rate*:** 9600, 19200, 38400 ou 115200.
- ***Data Bits*:** 8.
- ***Parity*:** None.
- ***Stop Bits*:** 1.
- ***Flow Control*:** None.

Em alguns modelos de switches existe a possibilidade de alterar os parâmetros da porta serial de acesso da console. Na Figura 16 um exemplo do switch Edge-core modelo ECS2100-28T que possui a possibilidade de alterar os parâmetros de configuração da porta de console.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

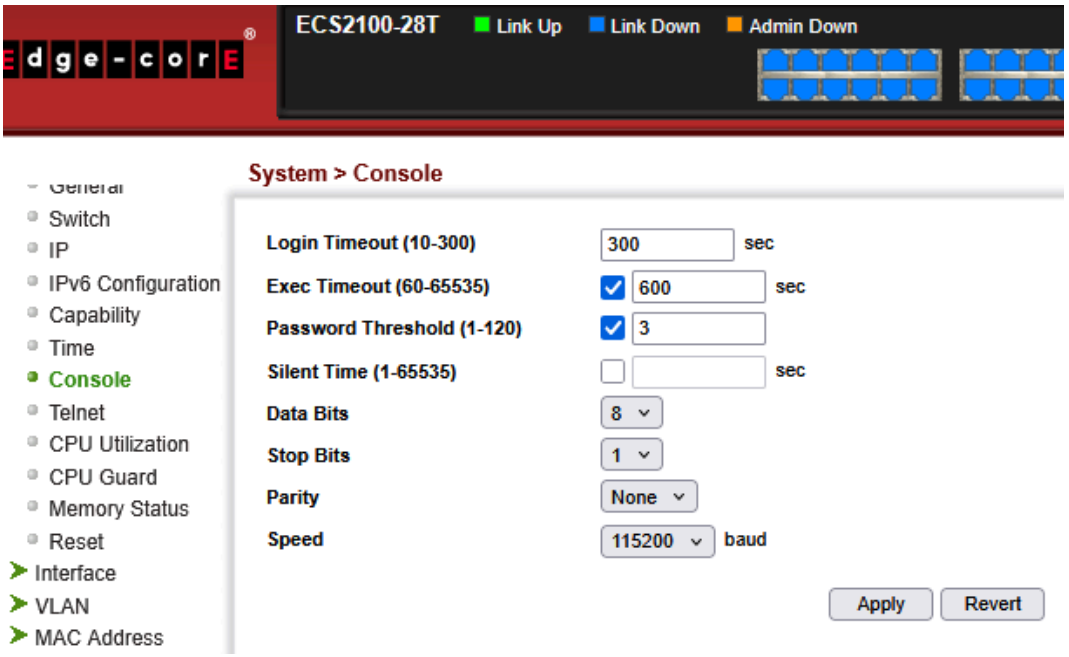


Figura 16. Configurações da porta de console.

É altamente recomendável verificar a documentação do switch específico e as configurações da portal serial, em caso da possibilidade de alteração de parâmetros, o qual está sendo realizado o acesso para confirmar as configurações corretas da porta de console. Como exemplos de softwares de emulação de terminal dois dos mais populares são o Putty (https://www.putty.org/) e o Tera Term (https://teratermproject.github.io/). Em sistemas operacionais Linux o utilitário Minicom (https://salsa.debian.org/minicom-team/minicom) é um dos meios mais utilizados para acesso a comunicação serial.

O PuTTY é um software de emulação de terminal gratuito e de código aberto, amplamente utilizado em sistemas operacionais Windows para estabelecer conexões seriais, SSH e Telnet. Para configurar uma conexão serial com um switch utilizando um cabo *rollover* no PuTTY, são necessários os seguintes passos:

1. Abrir o PuTTY.
2. Na janela de configurações, selecionar a opção "*Serial*" no painel esquerdo, em "Connection".
3. No campo "*Serial line to connect to*", inserir o nome da porta COM disponível no sistema operacional Windows (por exemplo, COM1, COM2) ou o caminho do dispositivo serial (por exemplo, /dev/ttyS0 no Linux). Se estiver utilizando um adaptador USB para serial, verificar o Gerenciador de Dispositivos (no Windows) ou a pasta /dev (no Linux/macOS) para identificar a porta correta.
4. No campo "*Speed (baud)*", inserir a velocidade de transmissão (*baud rate*) configurada para a porta de console do switch (geralmente 9600).

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

5. Verificar se as opções "*Data bits*" estão definidas como 8, "*Stop bits*" como 1 e "*Parity*" como *None*, a menos que a documentação do switch especifique o contrário.
6. Certificar de que a opção "*Flow control*" esteja definida como "*None*".
7. Clicar no botão "*Open*" para iniciar a conexão serial com o switch.

O Tera Term é outro software de terminal gratuito e popular, especialmente para usuários do sistema operacional Windows, que suporta conexões seriais, SSH e Telnet. Para configurar uma conexão serial no Tera Term:

1. Abrir o Tera Term.
2. Na janela "*Tera Term: New Connection*", selecionar a opção "Serial".
3. No menu suspenso "*Port*", selecionar a porta COM correspondente à conexão serial (porta serial nativa ou porta do adaptador USB para serial).
4. Configurar os parâmetros de conexão (*Baud rate, Data bits, Parity, Stop bits*) de acordo com as especificações do switch.
5. Clicar no botão "OK" para estabelecer a conexão.

No caso do uso de adaptadores USB para serial, após a instalação dos *drivers*, o adaptador USB para serial será reconhecido pelo sistema operacional como uma porta COM virtual (no Windows) ou um dispositivo serial em /dev (no Linux/macOS). Para utilizar o software de terminal com o adaptador, é necessário identificar essa porta COM ou dispositivo serial e selecioná-lo nas configurações de conexão serial do software. No Windows, essa informação pode ser encontrada no Gerenciador de Dispositivos, na seção "Portas (COM e LPT)". Em sistemas Linux e macOS, o dispositivo serial geralmente aparece como um arquivo em /dev/ttyUSBx ou /dev/ttyACMx. Na Figura 17, há um exemplo de cabo USB para serial.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Figura 17. Cabo USB para serial;

2.3 Solução de Problemas Comuns

Ao tentar acessar a console de um switch com um cabo *rollover*, alguns problemas comuns podem ocorrer:

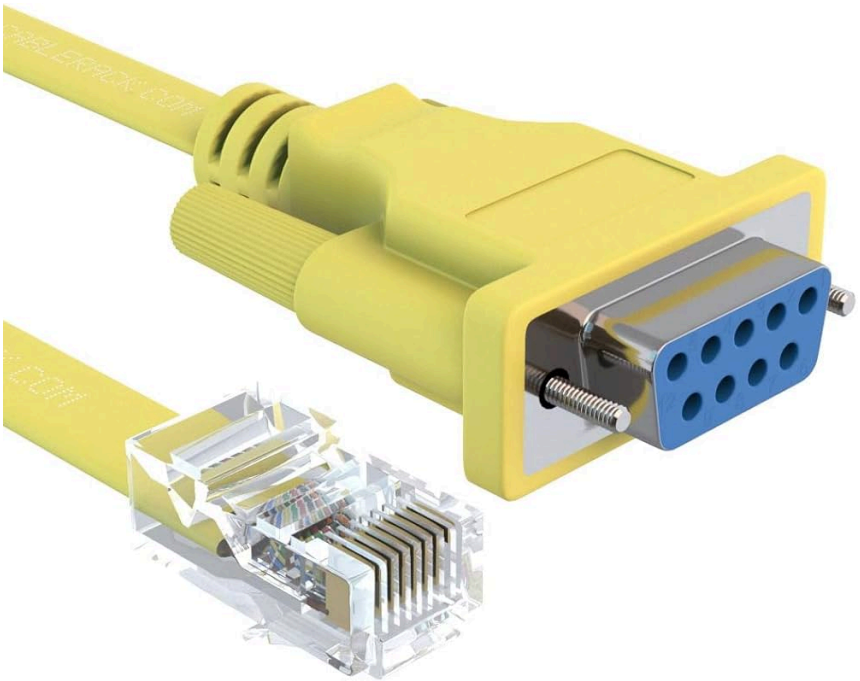
- **Sem resposta na tela do terminal:** Verificar se o cabo *rollover* está corretamente conectado tanto ao switch quanto ao computador. Certificar de que as configurações do software de terminal (baud rate, data bits, paridade, stop bits, controle de fluxo) correspondem às configurações da porta de console do switch. Se estiver sendo utilizado um adaptador USB para serial, verificar se a porta COM selecionada no software de terminal é a correta e se os drivers do adaptador estão instalados e funcionando.
- **Saída ilegível ou caracteres estranhos:** Esse problema geralmente indica uma incompatibilidade nas configurações de velocidade (baud rate), bits de dados, paridade ou bits de parada entre o computador e o switch. Verificar novamente a documentação do switch para confirmar as configurações corretas e ajustar no software de terminal.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

- **Problemas com drivers do adaptador USB para serial:** Se a conexão não funcionar, pode haver um problema com os *drivers* do adaptador. Tentar reinstalar ou atualizar os *drivers* seguindo as instruções do fabricante do adaptador.
- **Porta de console desabilitada no switch:** Em alguns casos, a porta de console pode estar desabilitada por configuração. Isso geralmente requer outros métodos de acesso inicial ao switch (como conexão via porta de gerenciamento ou redefinição para as configurações de fábrica) para reabilitar a porta de console.

2.4 Tipos de Cabo

Um cabo *rollover*, também conhecido como cabo Yost, cabo Cisco ou cabo de console, é um tipo específico de cabo *null-modem* utilizado para conectar um computador diretamente à porta de console de um switch. A principal finalidade deste cabo é permitir o acesso à interface de linha de comando (CLI) do dispositivo, o que é necessário para realizar tarefas de configuração, monitoramento e solução de problemas. A característica distintiva de um cabo *rollover* reside na sua pinagem interna: os fios em uma extremidade do cabo são conectados de forma reversa em relação à outra extremidade, como se o cabo plano tivesse sido "rolado". Essa configuração particular permite uma comunicação serial direta entre o computador e o switch, sendo fundamental para o acesso *out-of-band* (fora do canal de comunicação padrão). Na Figura 18, um cabo *rollover* com um conector RJ45 em uma ponta e um conector DB9 na outra extremidade.



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Figura 18. Conexões em um cabo *rollover*.

Uma configuração comum para conectar um computador à porta de console de um switch é utilizando um cabo *rollover* com um conector RJ45 em uma extremidade (para conectar ao switch) e um conector DB9 fêmea na outra extremidade (para conectar à porta serial do computador). A correspondência dos pinos entre esses dois conectores é necessária para o funcionamento da conexão. A Tabela 7 apresenta uma pinagem comum para essa configuração, incluindo os sinais de cada pino. Esta configuração é amplamente utilizada em muitos switches, especialmente modelos mais antigos. No entanto, pequenas variações podem existir dependendo do fabricante e do modelo específico do switch.

Tabela 7: Pinagem Comum do Cabo Rollover RJ45 para DB9

Pino RJ45	Sinal	Pino DB9
1	CTS	8
2	DSR	6
3	RXD	2
4	GND	5
5	GND	5
6	TXD	3
7	DTR	4
8	RTS	7

2.5 Configurações de Fábrica

A restauração de um switch para as configurações de fábrica pode ser necessária em diversas situações, como solucionar problemas de configuração, preparar um switch para ser utilizado em uma nova rede ou apagar configurações antigas antes de descartar o equipamento.

Existem vários métodos para restaurar um switch para as configurações de fábrica, e o método específico pode variar dependendo do fabricante e do modelo. Um método comum envolve o uso de um botão de reset físico, geralmente localizado na parte frontal ou traseira do switch. O procedimento típico é desligar o switch, pressionar e segurar o botão de reset por um determinado período (que pode variar de alguns segundos a mais de 10 segundos, conforme indicado na documentação do fabricante), e então religar o switch.

Outro método comum é através da interface de linha de comando (CLI), acessada via console. Comandos como "*erase startup-config*" (que apaga a configuração salva) seguido de "*reload*" (que reinicia o switch) são frequentemente utilizados em switches Cisco. Alguns fabricantes podem ter comandos equivalentes ou ligeiramente diferentes. Os switches com interface de gerenciamento web oferecem uma opção para restaurar as configurações de fábrica através do menu de administração ou manutenção. Na Figura 19, um acesso por

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

console para ativar opção para restauração das configurações de fábrica em um switch Linksys modelo SRW224G4.

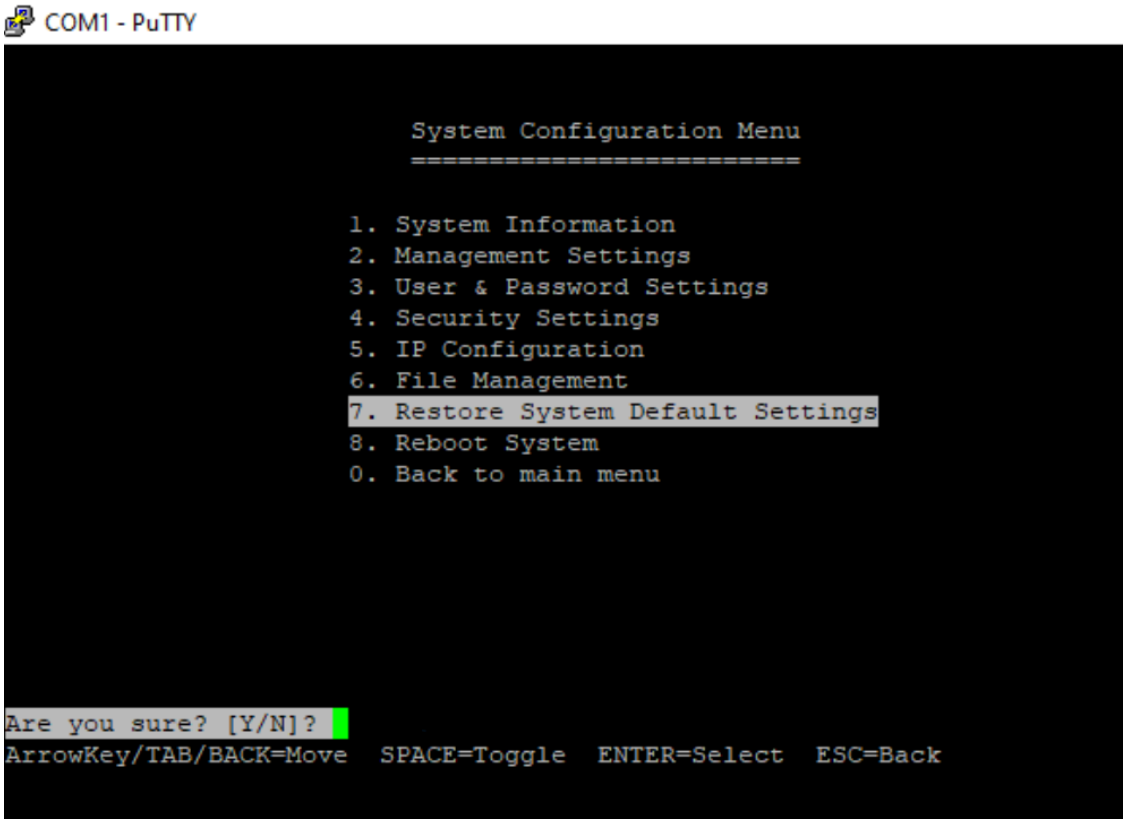


Figura 19. Opção para restauração das configurações de fábrica

2.6 Interface de Gerenciamento

As conexões serial (RS-232) e USB são os métodos primários para obter acesso local à console de um switch. Esses métodos são os recomendados para a configuração inicial do dispositivo e para cenários onde o acesso via rede ainda não está disponível ou foi perdido. Além dessas conexões diretas, existem outras formas de acessar a interface de gerenciamento de um switch, como Telnet, SSH (*Secure Shell*) e a interface web (HTTP/HTTPS). No entanto, esses métodos geralmente requerem que o switch já tenha sido configurado com um endereço IP e que os serviços correspondentes estejam habilitados, o que muitas vezes é realizado inicialmente através da conexão de console.

Os protocolos Telnet e SSH proporcionam acesso remoto à linha de comando, sendo o SSH preferível por oferecer uma conexão criptografada e mais segura. A interface web permite o gerenciamento do switch através de um navegador, oferecendo uma interface gráfica que pode ser mais intuitiva para alguns usuários.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Ao acessar um switch pela primeira vez, seja através da console ou da interface web, geralmente são necessárias credenciais de autenticação padrão. Os fabricantes de switches frequentemente definem um nome de usuário e uma senha padrão para permitir o acesso inicial aos seus dispositivos. Essas credenciais variam dependendo do fabricante e, por vezes, do modelo específico do switch. Algumas das combinações padrão mais comuns incluem "admin" para nome de usuário e "admin" para senha , "cisco" para ambos , ou, em alguns casos, o nome de usuário pode ser "admin" e a senha pode ser deixada em branco. É uma boa prática consultar a documentação fornecida pelo fabricante para obter as credenciais padrão específicas do modelo do switch em questão.

A utilização dessas credenciais padrão representa um risco de segurança significativo, pois são informações publicamente conhecidas. Portanto, é fundamental alterar essas credenciais imediatamente após o primeiro acesso ao switch para senhas fortes e exclusivas. A Tabela 8 fornece uma referência rápida das credenciais padrão mais comuns utilizadas por diferentes fabricantes de switches.

Tabela 8. Credenciais e endereços comuns em switches gerenciáveis.

Fabricante	Nome de Usuário Padrão	Senha Padrão	Endereço IP Padrão (Comum)
Cisco	cisco / admin	cisco / admin	192.168.1.1 / 192.168.1.254
TP-Link	admin	admin	192.168.0.1
Linksys	admin	admin	192.168.1.251
Aruba (HPE)	admin	(em branco)	192.168.1.1 / 169.254.x.x
FS.com	admin	admin	192.168.1.1
Netgear	admin	qscsystems	192.168.0.110 / 192.168.0.120 / 192.168.0.121
Sophos	(varia)	(varia)	172.16.16.239
SonicWall	(varia)	(varia)	192.168.168.169

A forma como um switch obtém um endereço IP na sua configuração inicial pode variar. Muitos switches são configurados para tentar obter um endereço IP automaticamente através do protocolo DHCP. Se um servidor DHCP estiver presente na rede, o switch receberá um endereço IP, máscara de sub-rede e gateway padrão. No entanto, se não houver um servidor DHCP disponível ou se o switch não conseguir obter um endereço dessa forma, ele geralmente utilizará um endereço IP estático padrão pré-configurado pelo fabricante. Alguns endereços IP padrão comuns incluem 192.168.0.1, 192.168.1.1, 192.168.1.251 e 169.254.x.x (onde os dois últimos octetos são derivados do endereço MAC do switch). A documentação do fabricante ou uma etiqueta no dispositivo geralmente indicam o endereço IP padrão. Se essa informação não estiver prontamente disponível, pode-se tentar fazer um ping em alguns

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

dos endereços padrão mais comuns a partir de um computador conectado à mesma rede local. Em muitos casos, se o switch não conseguir obter um endereço IP via DHCP, a configuração inicial através da conexão de console serial será necessária para definir um endereço IP estático e as outras configurações de rede.

2.7 Acesso remoto

Os métodos de acesso remoto mais comuns em switches são com os protocolos Telnet, SSH e HTTP/HTTPS por meio de uma interface web.

Telnet

O Telnet é um protocolo de rede que permite o acesso remoto à linha de comando de um switch através de uma rede IP, operando tipicamente na porta TCP 23. Este método requer que o switch tenha um endereço IP já configurado em uma de suas interfaces, geralmente uma interface na VLAN de gerenciamento. Para o acesso inicial via Telnet, os switches frequentemente vêm com endereços IP padrão, como 192.168.0.1 ou 192.168.1.1. Esses endereços padrão simplificam o acesso inicial baseado em rede, mas representam um risco de segurança significativo se não forem prontamente alterados para endereços mais seguros e exclusivos.

Uma grande preocupação de segurança com o Telnet é que ele transmite todos os dados, incluindo nomes de usuário e senhas, em texto plano, tornando-o suscetível à interceptação e leitura do tráfego gerado pelo protocolo na rede. Devido a essas vulnerabilidades de segurança, o Telnet geralmente não é recomendado para ambientes de produção e deve ser usado apenas em ambientes isolados e em VLANs de gerenciamento.

O serviço Telnet é tipicamente desabilitado por padrão em muitos switches modernos e deve ser explicitamente habilitado através da console ou outra interface de gerenciamento segura antes que as conexões Telnet possam ser estabelecidas. A prática comum de usar endereços IP padrão para dispositivos de rede cria uma vulnerabilidade de segurança generalizada. Os administradores de rede devem priorizar a alteração dessas configurações padrão imediatamente após o acesso inicial para evitar acesso não autorizado e potenciais violações de segurança.

SSH (Secure Shell)

O protocolo SSH fornece uma alternativa segura ao Telnet para acesso remoto à linha de comando de switches. O SSH criptografa toda a comunicação entre o cliente e o switch, garantindo a confidencialidade e a integridade dos dados transmitidos. Ele tipicamente usa a porta TCP 22. Vários softwares de emulação de terminal, incluindo os amplamente utilizados PuTTY e Tera Term, suportam conexões SSH.

Semelhante ao Telnet, o serviço SSH geralmente precisa ser habilitado no switch antes que conexões remotas possam ser estabelecidas. Habilitar o SSH geralmente envolve a geração de chaves SSH no switch para autenticação segura. Em switches mais antigos

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

poderá haver incompatibilidades dos métodos criptográficos com os clientes de SSH mais atuais. Nestes casos, deverá ser usado uma versão de cliente de SSH mais antigo ou habilitar os métodos legados de criptografia para realizar o acesso ao switch.

Protocolo SSH - https://youtu.be/bh7DwPtYkrY

Web GUI (Graphical User Interface)

Um número significativo de switches apresenta uma interface de gerenciamento baseada na web, acessível através de um navegador da web padrão usando HTTP ou o protocolo HTTPS. Acessar a console web requer que o switch tenha um endereço IP configurado e os serviços HTTP ou HTTPS habilitados.

A console web normalmente oferece uma interface visual amigável para configurar vários parâmetros, monitorar o desempenho e gerenciar as configurações de rede, tornando-o particularmente acessível para administradores de rede que preferem uma abordagem gráfica em vez da interação pela linha de comando. No entanto, é importante notar que certos recursos de gerenciamento avançados ou menos comumente usados podem estar disponíveis apenas através da interface de linha de comando. Outra questão está relacionada a aplicação de comandos na interface web, que em vários casos dará mais trabalho para o administrador de redes do que realizando as configurações em linha de comando.

Em alguns switches mais antigos, que faziam uso do Adobe Flash ou alguma tecnologia legada na interface web, o acesso deve ser feito com versões de navegadores antigos, por exemplo com o uso de Internet Explorer 5 em um Microsoft Windows XP. Para estes casos é necessário o uso de máquinas virtuais para obter acesso ao console web do switch.

Outras alternativas

Existem outros métodos de acesso remoto com ferramentas proprietárias fornecidas pelo próprio fabricante do switch ou por terceiros. Um dos exemplos é o *Omada Software Controller* (https://www.omadanetworks.com/br/omada-sdn) da TP-Link que serve como uma plataforma de gerenciamento centralizada para dispositivos habilitados para a plataforma *Omada*, incluindo switches. O *Omada Controller* fornece recursos como acesso à nuvem, monitoramento de rede e gerenciamento de configuração, que podem facilitar o acesso à console ou fornecer funcionalidades de gerenciamento equivalentes através de sua interface. Entretanto, é uma solução proprietária e para uso em dispositivos da fabricante TP-Link.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

2.8 Leds de Indicação

Os LEDs indicadores em switches fornecem informações importantes sobre o status e a atividade do dispositivo e de suas portas. Geralmente, há LEDs para indicar o status da energia, a atividade da rede e a velocidade da conexão. Na Figura 20, um exemplo de leds indicando atividade em portas de um switch.

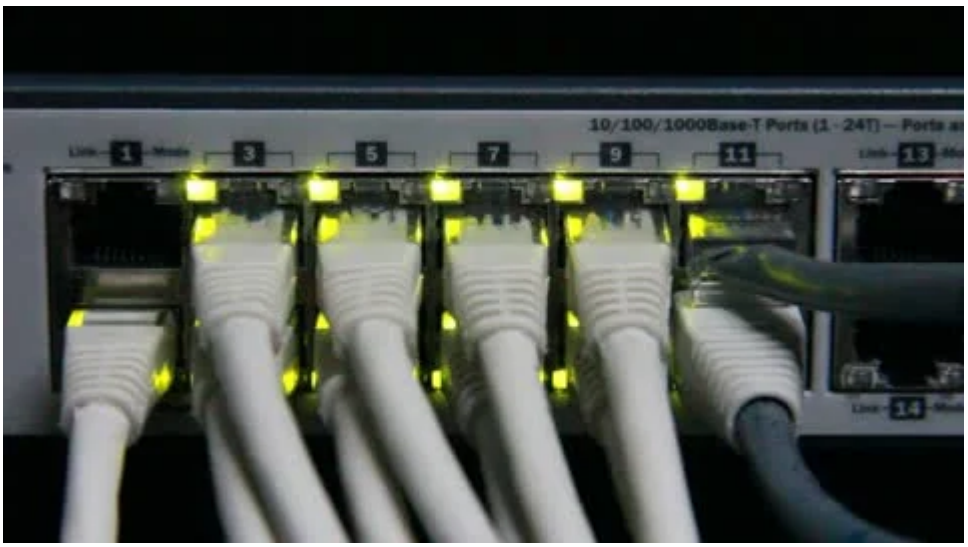


Figura 20. LEDs em atividade em portas de um switch.

Para as portas individuais, muitos switches possuem dois LEDs por porta. Um LED geralmente indica o status do link e a velocidade da conexão, enquanto o outro indica a atividade. Por exemplo, um LED pode acender em verde para indicar uma conexão de 100 Mbit/s e em âmbar para uma conexão de 1 Gbit/s. Se o LED estiver piscando, geralmente indica que há tráfego de dados passando por essa porta. A ausência de luz pode indicar que não há conexão ou que a porta está administrativamente desativada. Alguns switches mais recentes podem usar cores diferentes, como azul ou branco, para indicar diferentes status, como inicialização, atualização de firmware ou conexão à nuvem.

Além dos LEDs de porta, os switches também podem ter LEDs de status para a fonte de alimentação (PSU), ventiladores (*coolers*) e o sistema geral. Um LED verde sólido geralmente indica operação normal, enquanto um LED âmbar piscando pode indicar uma falha ou problema. A velocidade de piscar também pode fornecer informações adicionais sobre a gravidade ou o tipo de problema. Por exemplo, em caso de loop físico na rede, todos os leds ativos nas portas do switch deverão ficar piscando em sincronia, resultado do alto volume de tráfego. Consultar a documentação do fabricante para o modelo específico do switch é sempre recomendado para entender completamente o significado de cada LED.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

2.9 Identificação das portas

A identificação física das portas dos switches obedecem uma ordem numérica, normalmente, começando em 1 até o número total de portas disponíveis. Entretanto, não há um padrão sobre disposição das portas em relação ao número, por exemplo, se a numeração será da parte superior da esquerda para a direita em ordem crescente ou será a partir da parte superior. Portanto, é importante observar os números impressos nas portas para ter certeza de qual porta é a correta. Na Figura 21, um exemplo do switch Huawei modelo S5735-L24P4S-A1, que possui um padrão de numeração menos comum, sendo a porta de número 1 na parte inferior do bloco de portas.

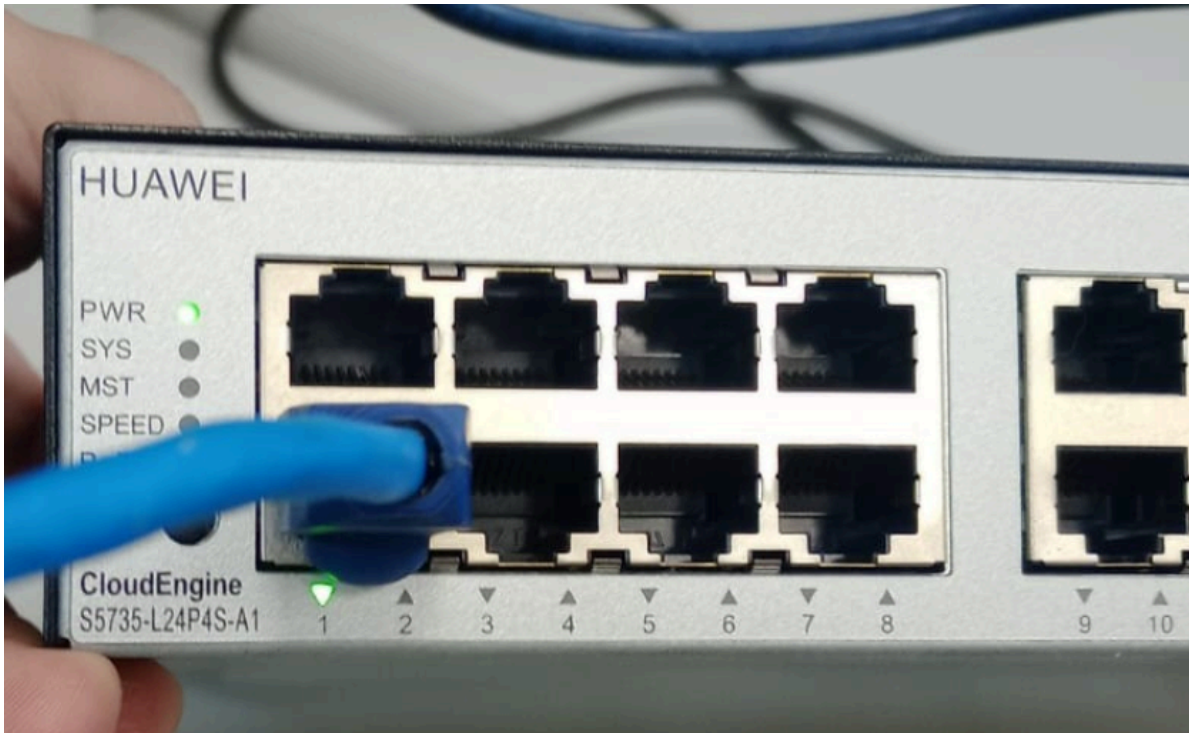


Figura 21. Identificação das portas em um switch Huawei S5735-L24P4S-A1

As identificações das portas na aplicação de comandos e configurações podem ter outras nomenclaturas. É comum em equipamentos que possuem a interface em linha de comando identificar as portas com o tipo de interface, numeração de *slot* ou *chassi* e um número decimal. Por exemplo, a identificação f0/1 indicaria uma porta Fast Ethernet (10/100 Mbit/s) na porta física 1 em um switch Cisco sem módulos removíveis. Na Tabela 9, mais alguns exemplos de identificação de portas comuns em switches que possuem linhas de comando.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Tabela 9. Exemplos de identificações de interfaces

Nome da Porta	Descrição
f0/1	Fast Ethernet, switch fixo (módulo 0 implícito), porta 1
gi1/0/2	Gigabit Ethernet, módulo 1, sub-módulo/placa 0, porta 2.
te0/0/1/0	Ten Gigabit Ethernet, switch fixo (módulo 0 implícito), sub-módulo/placa 0, porta 1, sub-porta 0 (alguns sistemas podem ter sub-portas em interfaces de alta densidade)
SFP1/2	Porta SFP no módulo 1, porta 2
Port-channel1	Interface lógica de agregação de links número 1
Vlan10	Interface virtual associada à VLAN 10

2.10 Racks

A maioria dos switches é projetada para ser instalada em racks de equipamentos padrão de 19 polegadas. Esses racks oferecem uma solução organizada para montar múltiplos dispositivos, otimizando o espaço e facilitando o gerenciamento de cabos e o fluxo de ar.

A altura dos racks é medida em unidades "U", onde 1 U corresponde a 1,75 polegadas (44,45 mm). Ao planejar a instalação, é importante determinar a altura em U do switch e de outros equipamentos a serem montados no rack para garantir que haja espaço suficiente disponível. A escolha do tipo de rack depende das necessidades de densidade, estabilidade e acesso aos equipamentos. Os tamanhos comuns de racks são 8U, 9U, 12U, 24U e 44U, com profundidades variáveis que vão de 450mm a 650mm. Na Figura 22, um rack de 8U para uso em parede.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Figura 22. Rack de 8U para uso em parede

Os racks de piso oferecem maior estabilidade para equipamentos mais pesados. Os racks de parede são recomendados para uso com 12U de altura e o peso utilizado poderá necessitar de um suporte adicional para sustentação, por exemplo com o uso de um suporte em formato de “L” (mão francesa).

A maioria dos switches é fornecida com kits de montagem que incluem trilhos (ou suportes laterais) e parafusos. O primeiro passo é fixar os trilhos ou suportes nas laterais do switch, alinhando-os com os orifícios apropriados e utilizando os parafusos fornecidos no kit. Em seguida, o switch com os suportes fixados é elevado e alinhado com os orifícios correspondentes na estrutura do rack. Parafusos de rack adequados (geralmente do tipo 10-32 ou 12-24, dependendo do rack) são então utilizados para fixar os suportes do switch ao rack. É importante apertar os parafusos de forma segura, mas sem excesso de força para evitar danos à rosca ou ao equipamento.

Uma organização eficiente dos cabos é essencial para manter a ordem no rack, facilitar a manutenção e garantir um bom fluxo de ar. É recomendado que se considere uma folga de 40% do espaço como reserva para uso futuro ao se instalar um rack. É fundamental identificar todos os cabos com etiquetas em ambas as extremidades, indicando a origem e o destino. A utilização de organizadores de cabos horizontais e verticais dentro do rack ajuda a evitar emaranhados e mantém os cabos arrumados. Recomenda-se o uso de abraçadeiras de velcro em vez de abraçadeiras plásticas, pois as de velcro podem ser facilmente reaproveitadas e ajustadas para futuras alterações. Ao instalar os cabos, é importante deixar uma folga para permitir o movimento dos dispositivos durante a manutenção. Na Figura 23, um exemplo de rack montado com indicação dos componentes comuns em uma instalação de rede corporativa.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

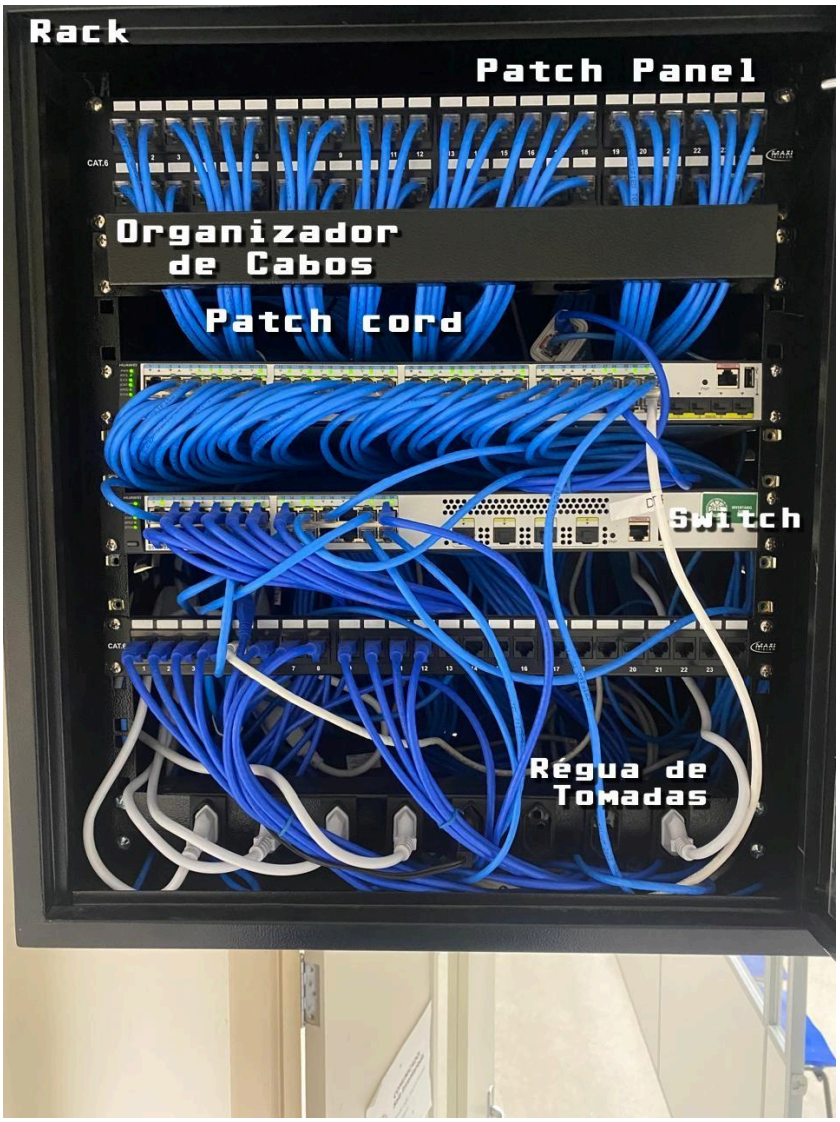


Figura 23. Rack montado.

Deve-se evitar o roteamento de cabos em locais que possam bloquear o acesso a outros equipamentos ou obstruir as entradas e saídas de ar dos switches. Por fim, manter uma documentação detalhada de todas as conexões de cabos é importante para facilitar o gerenciamento e a solução de problemas da rede. Uma boa organização de cabos não só melhora a estética, mas também facilita a manutenção, o fluxo de ar e a identificação de problemas.

Redes para Iniciantes - Racks - https://youtu.be/ukrG4q0usE4

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

2.11 Considerações para a Instalação Física de Switches

A etapa inicial para uma instalação bem-sucedida de um switch envolve uma análise cuidadosa de diversos fatores que podem influenciar o desempenho, a vida útil do dispositivo e a disponibilidade da rede.

A localização adequada para um switch deve priorizar a acessibilidade para manutenção e solução de problemas. É essencial considerar o espaço físico disponível, especialmente em ambientes onde os switches serão montados em racks. Locais com alta umidade, poeira excessiva ou temperaturas extremas devem ser evitados, pois essas condições ambientais podem prejudicar os componentes eletrônicos sensíveis do switch.

O planejamento do roteamento dos cabos é outro aspecto crítico, visando evitar obstruções ao fluxo de ar e facilitar futuras expansões ou alterações na rede. Em racks de parede que ficam instalados em corredores, onde não há climatização, é importante manter a taxa de ocupação do rack com folga de 40% e utilizar exaustores para amenizar a temperatura interna.

A localização do rack deve ser planejada para não estar vulnerável a acesso não permitido e que esteja em condições de ser usado com tranquilidade em casos de manutenção em switches e cabeamento. Por exemplo, colocar um rack a 5 metros de altura dificulta o acesso não autorizado de pessoas, entretanto, complica muito a prestação de manutenção no local. Ao projetar uma rede deve-se posicionar os racks com o menor roteamento de cabos possível e distribuir os pontos de rede de forma a não sobrecarregar racks de parede. Nestes casos, poderá haver a necessidade de trocar um rack em produção, algo que poderá ser bem complexo e consumir um tempo considerável para ser realizado.

A ventilação adequada é fundamental para dissipar o calor gerado pelo switch durante sua operação, prevenindo o superaquecimento e prolongando sua vida útil. Existem diferentes tipos de fluxo de ar em switches, incluindo frontal para traseiro (onde o ar frio entra pela parte frontal, próxima às portas de rede, e sai pela parte traseira, perto da fonte de alimentação), traseiro para frontal (o inverso do anterior) e lateral para lateral. É fundamental alinhar o padrão de fluxo de ar do switch com o sistema de resfriamento do ambiente onde ele será instalado.

A alimentação de energia correta e estável é vital para a operação contínua de um switch. É necessário verificar os requisitos de energia específicos do dispositivo, tais como voltagem e corrente, e garantir que a fonte de alimentação seja adequada. Para ambientes que demandam alta disponibilidade, muitos switches oferecem a opção de fontes de alimentação redundantes. Devem ser usados *no-breaks* para evitar que as quedas de energia façam reinicializações nos switches Dependendo do modelo de switch e do firmware utilizado, o tempo de um *reboot* poderá chegar a vários minutos, conforme listado na Tabela 10, até o retorno ao funcionamento normal.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Tabela 10. Tempo de inicialização em switches diversos.

Fabricante	Modelo	Tempo de boot
Huawei	S5720	Aprox. 7 min
HP	1910	Aprox. 3 min
Cisco	WS-3560G-48TS	Aprox. 3,25 min
HP	1930	Aprox. 2 min
Cisco	2960	De 2 a 5 min
MikroTik	Série CRS3xx	De 00:45 a 02:00

Uma tecnologia importante a considerar é o *Power over Ethernet* (PoE) , que permite transmitir energia elétrica juntamente com os dados através do mesmo cabo Ethernet, simplificando a instalação de dispositivos como telefones IP, câmeras de segurança e *access points*. Ao utilizar PoE, é fundamental verificar se o switch oferece suporte ao padrão PoE necessário (por exemplo, IEEE 802.3af, 802.3at, 802.3bt) e qual o orçamento total de energia disponível para os dispositivos conectados.

O uso de no-breaks é altamente recomendado para proteger os switches contra interrupções no fornecimento de energia, garantindo a continuidade da operação da rede durante blecautes e prevenindo danos aos equipamentos causados por picos de tensão. O uso de *no-breaks* em rack de parede é um desafio devido ao peso adicional. Uma das formas de reforçar o rack de parede se faz com o uso de suporte metálicos em formato de “L” (mão francesa) na parte inferior do rack. Outra forma é criar uma rede elétrica dedicada para os racks, com o uso de *no-break* de maior potência que tenha capacidade de entregar a energia necessária para todos os racks da rede. Esta forma deve ser incluída no projeto elétrico de um prédio, no caso de construção de um novo prédio, por exemplo.

2.12 Ferramentas auxiliares

Ao realizar a instalação física de um switch novo os procedimentos disponíveis na documentação devem ser seguidos. Em casos de dúvida sempre verificar as atualizações da documentação no site do fabricante, isto facilitará bastante o processo de instalação. Se não houver impedimentos, a recomendação é partir de um estado conhecido das configurações padrão de fábrica. Entretanto, no caso de um switch antigo sem documentação ou um switch já configurado que esteja remoto devem ser usadas ferramentas auxiliares para identificação e acesso ao switch.

Uma informação importante do switch é o endereço MAC (endereço físico). Se este endereço for conhecido será possível encontrar o endereço IP do switch por meio da tabela ARP de um host na mesma rede. Para isto pode-se executar uma ferramenta de escaneamento na rede tais como nmap (https://nmap.org) ou arp-scan (https://github.com/royhills/arp-scan). Outra forma de descobrir o switch na rede é realizar buscas de endereços IP padrão do modelo em questão. Se o switch estiver com a

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

configuração de fábrica, poderá ser encontrado. Para isto, deve ser configurado um IP da mesma rede no host e realizar acessos por ping ou via navegador no IP padrão do switch. Se houver mais de um IP respondendo, na tabela ARP houver endereços MAC diferentes para o mesmo IP, pode-se fixar um dos endereços MAC encontrados para o IP padrão e realizar as configurações. Após, alterar para outro endereço MAC e realizar as configurações. Para fixar um endereço MAC para um IP utilizar o comando arp com o parâmetro "-s", por exemplo **arp -s 192.168.1.1 00-0A-EB-62-16-F9**

arp-scan - https://www.youtube.com/watch?v=jXcbOZPcPDM

ARP Estático - Acesso a dispositivos com o mesmo endereço IP - https://youtu.be/JqQsMz9WIfU

Outra forma de descoberta é com o uso do protocolo LLDP (*Link Layer Discovery Protocol*) que realiza a descoberta de dispositivos vizinhos e provê informações tais como nome do dispositivo, VLAN, IP de gerenciamento, tempo de atividade entre outras. A partir de um switch compatível com LLDP ou com um software cliente de LLDP em um sistema operacional Linux, pode-se identificar equipamentos remotos. Com a ferramenta de análise de tráfego Tcpdump pode-se utilizar um filtro para o protocolo LLDP desta forma **tcpdump -nn -i enp0s31f6 ether proto 0x88cc**, onde "**enp0s31f6**" é a interface conectada na rede do switch que está sendo identificado.

tcpdump - https://www.youtube.com/watch?v=1LUk6fw6W6M

A ferramenta Wireshark possui funcionalidades de análise de pacotes e provê um interpretador (*dissector*) do protocolo LLDP. O filtro de captura para o protocolo é igual ao da ferramenta Tcpdump. Além do filtro de captura, o Wireshark possui um filtro de amostragem (*display filter*) específico para o protocolo que tem o nome de "**lldp**". Na Figura 24, um pacote LLDP que está sendo analisado na ferramenta Wireshark e onde pode ser visto o endereço IP usado na VLAN de gerenciamento de um switch Huawei.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

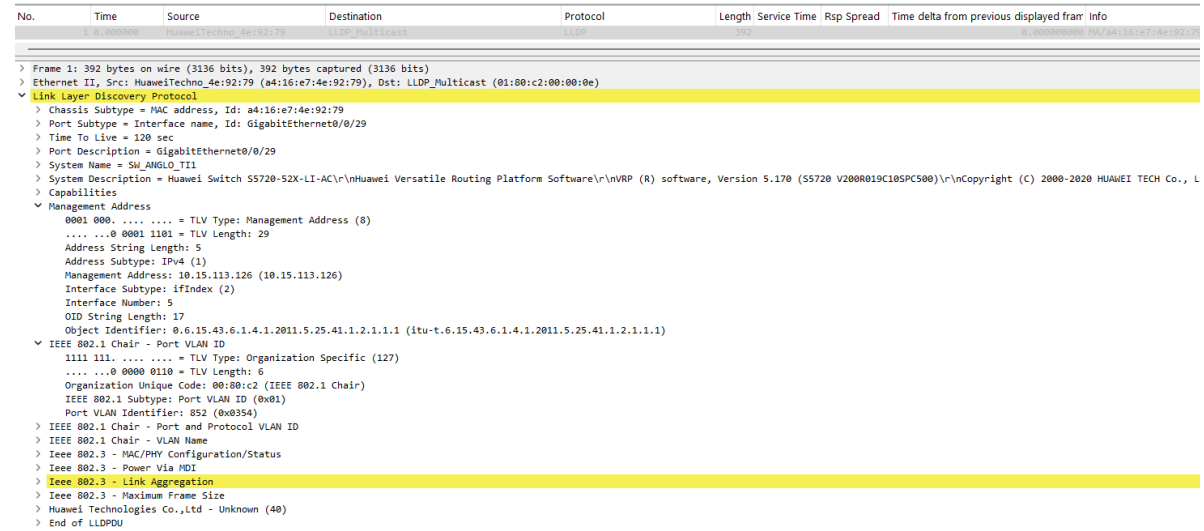


Figura 24. Pacote LLDP em análise na ferramenta WIreshark.

Se um switch não possuir o protocolo LLDP ou o protocolo estiver desabilitado, ainda há como achar o switch na rede pelo endereço IP padrão ou pelo endereço físico. Se o switch enviar pacotes em broadcast ou em multicast, é possível utilizar filtros de captura na ferramenta Tcpdump ou Wireshark. O filtro de captura para um endereço IP é "**host endIP**" onde o "**endIP**" deve ser substituído pelo endereço IP o qual os pacotes serão capturados. Para realizar capturas de pacotes para um determinado endereço físico utiliza-se o filtro "**ether host endMAC**", onde o "**endMAC**" deve ser substituído pelo endereço físico no formato XX:XX:XX:XX:XX:XX. Desta forma, se o switch se anunciar na rede poderá ser identificado o endereço IP de gerenciamento.

Wireshark - https://www.youtube.com/playlist?list=PLJE51qhGRWYVQbUMvf5yXlRrqMEiLOutW

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

3) Configurações Básicas

Este capítulo inicia a exploração das configurações fundamentais em switches gerenciáveis, no qual será abordada a configuração inicial que estabelece a identidade e o funcionamento básico do switch. O texto começará pela atribuição de um nome para fácil identificação e pela correta configuração de data e horário, importantes para a sincronização de eventos e logs. No prosseguimento, serão tratados o status e as características das Portas Metálicas e Portas de Fibra Óptica.

No decorrer do capítulo, a funcionalidade do logs para o diagnóstico de problemas e o rastreamento de eventos na rede, bem como a análise da tabela MAC, essencial para o encaminhamento de quadros Ethernet. Também a configuração do agente SNMP (*Simple Network Management Protocol*), um protocolo fundamental para o gerenciamento e monitoramento remoto do dispositivo será abordada.

Será explorado o LLDP (*Link Layer Discovery Protocol*), um protocolo de descoberta de vizinhos que facilita o mapeamento da topologia da rede. Ainda serão apresentados os controles de tráfego broadcast e multicast, mecanismos importantes para otimizar a utilização da largura de banda e prevenir a degradação do desempenho da rede.

Finalmente, o capítulo tratará de operações essenciais para a manutenção e a segurança do switch, como o backup e o restore da configuração, o processo de atualização de software (firmware) para garantir a disponibilidade de novas funcionalidades e correções de segurança, o uso de ferramentas de diagnóstico para identificar e solucionar problemas, e os procedimentos de reboot e restauração das configurações de fábrica (*Reset to Factory Defaults*) em diferentes cenários.

3.1 Nome (*Hostname*)

O nome (*hostname*) é um identificador textual único atribuído ao switch para facilitar o gerenciamento e a identificação na rede. É essencial para administração remota e diagnóstico. O nome não precisa ser registrado em um servidor de DNS, pode ter validade somente local. Em alguns switches o limite de tamanho de nome é bem restrito, portanto para criar um padrão de nomes para todos os switches é importante observar essa limitação. Uma dica para uso de nomes em switches está na localização e na funcionalidade do dispositivo. Por exemplo, **swPredio3-A1-R2** poderia ser usado para identificar o switch do prédio 3, no primeiro andar (A1) e que está instalado no rack R2. Na Tabela 11 estão exemplos da configuração em switches diversos.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Tabela 11. Exemplos da configuração em switches diversos.

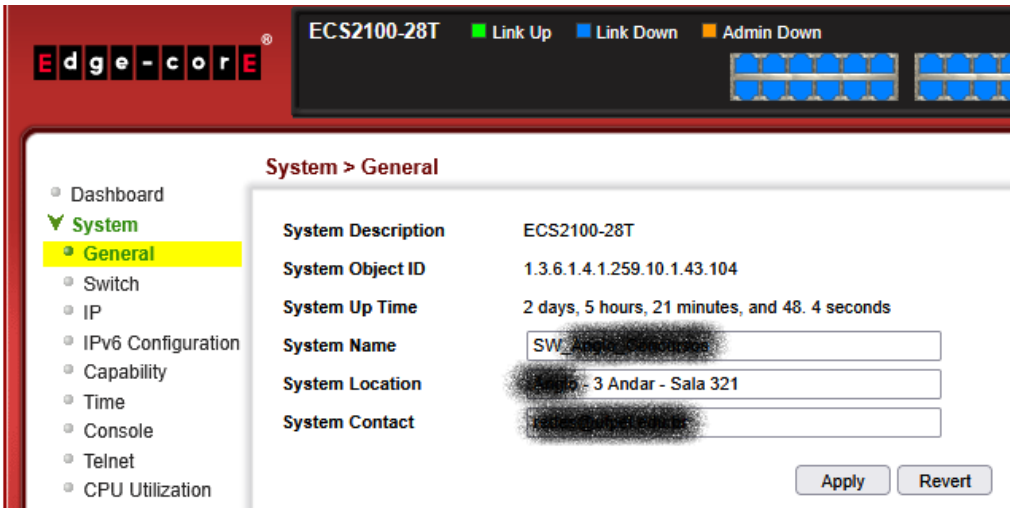
Cisco 2960 (CLI)

switch>enable
switch#conf t
switch(config)# hostname swPredio3-A1-R2

Huawei S5720-52X-LI (CLi)

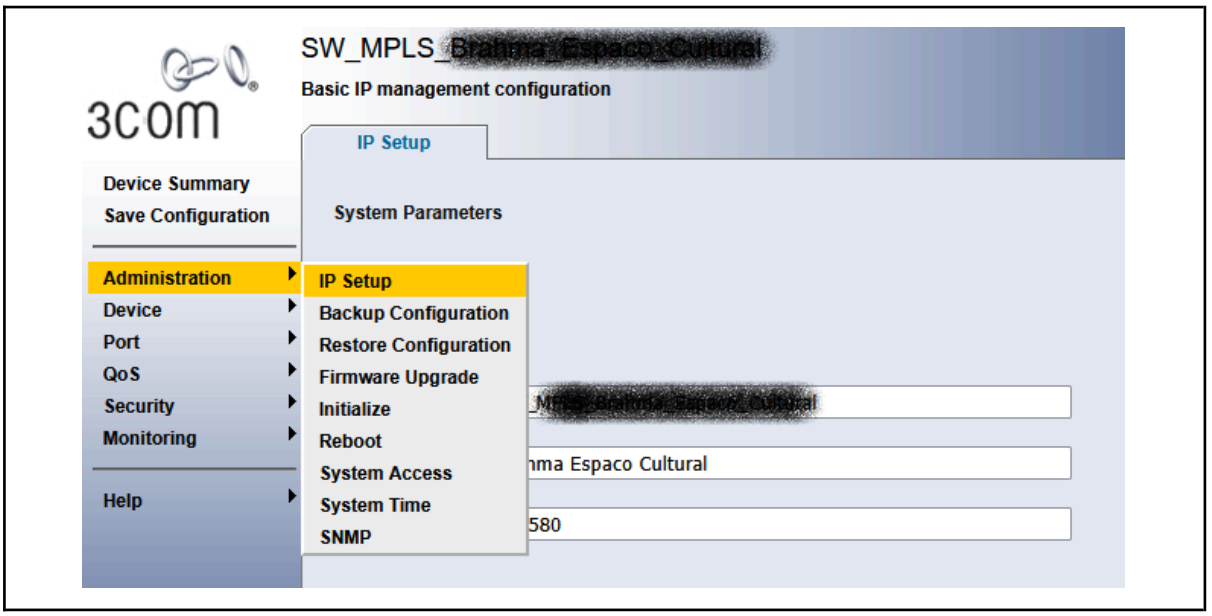
<switch> system-view
[switch] sysname swPredio3-A1-R2

Edgecore ECS2100-28T (Web)



3com 2226 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



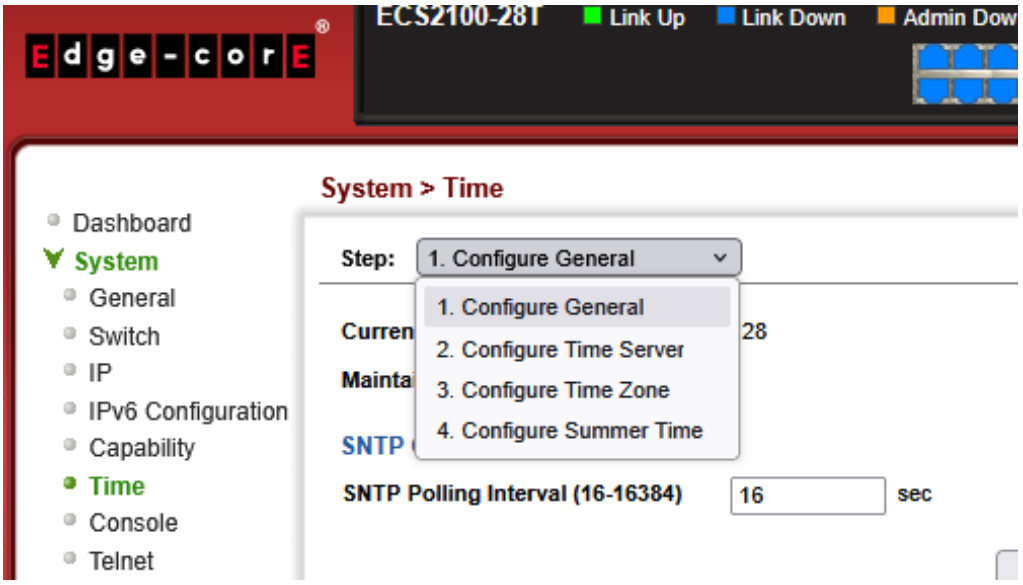
3.2 Data e Horário

As configurações de data, horário e *timezone* (zona de tempo) são essenciais para a correta marcação temporal de eventos nos logs, sincronização com servidores NTP (*Network Time Protocol)* e para o funcionamento adequado de alguns protocolos e funcionalidades. É recomendado que seja utilizado um servidor de NTP interno, na mesma VLAN de gerenciamento para evitar a conexão dos switches com serviços externos. Na Tabela 12 estão exemplos da configuração em switches diversos.

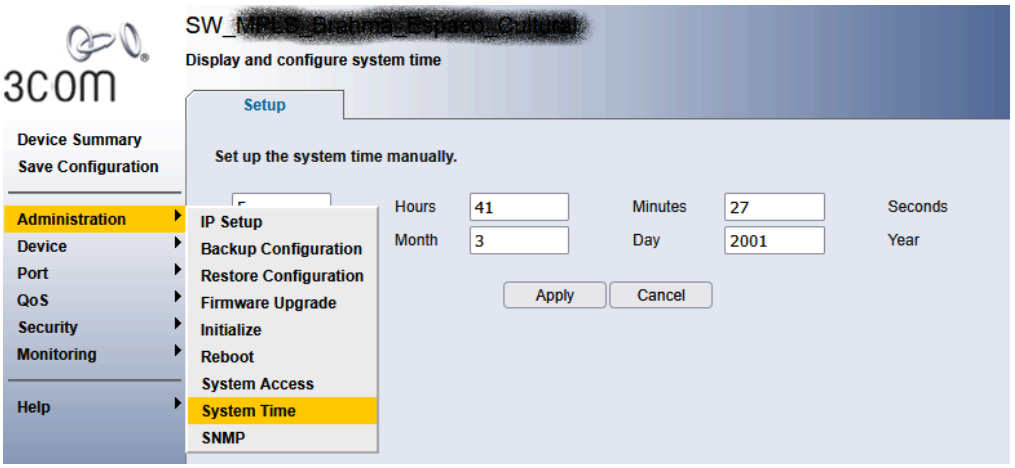
Tabela 12. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch#conf t* *switch(config)# ntp server **10.0.0.22*** *switch(config)# clock timezone GMT -3 0*
Huawei S5720-52X-LI (CLi) *<switch> clock timezone **brasil** minus 03:00:00* *<switch> system-view* *[switch] ntp-service unicast-server **10.0.0.22***
Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



3com 2226 (Web)



** Este modelo de switch não tem suporte ao protocolo NTP e ajuste de timezone.*

3.3 Portas Metálicas

As portas metálicas são as interfaces de conexão que utilizam cabos de par trançado terminados em conectores RJ-45. Estas portas suportam diferentes velocidades 10, 100, 1000 Mbit/s (Ethernet, Fast Ethernet, Gigabit Ethernet) e são as mais comuns em switches. Uma das funcionalidades primárias é a capacidade de configurar a velocidade e o modo de operação da porta. É possível definir manualmente a velocidade e o modo de duplex (*half-duplex* ou *full-duplex*). Essa configuração manual é muito útil em cenários onde a negociação automática pode falhar (*autonegotiation*), quando se deseja garantir uma configuração específica para compatibilidade com dispositivos mais antigos ou para otimizar o

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

desempenho. Em alguns casos pode-se desabilitar a porta de forma administrativa para evitar o uso indevido de conexões na rede.

Características

Os switches gerenciáveis oferecem funcionalidades de monitoramento e diagnóstico por porta. Estatísticas de tráfego em tempo real, contadores de erros, informações sobre o status do link e a capacidade de realizar testes de cabo diretamente nas portas auxiliam na identificação e resolução de problemas de conectividade. É uma boa prática utilizar um texto com a descrição da porta para informar qual a funcionalidade da porta, por exemplo "**UplinkPredio5**" ou algo relacionado ao dispositivo conectado, por exemplo "**Impressora1-ADM**".

Estatísticas

As estatísticas disponíveis por meio de contadores nas portas dos switches são importantes para auxiliar no diagnóstico de problemas nas conexões. Entre os contadores mais comuns estão:

- **Bytes e Pacotes Transmitidos (Tx)**: Indicam o volume total de dados (em bytes) e o número de pacotes enviados pela porta. Essas métricas ajudam a entender a carga de saída da porta.
- **Bytes e Pacotes Recebidos (Rx)**: Similarmente, mostram o volume total de dados e o número de pacotes recebidos pela porta, refletindo a carga de entrada.
- **Taxa de Transferência Atual (bit/s)**: Exibe a velocidade instantânea de transmissão e recepção de dados na porta.
- **Pacotes Broadcast/Multicast**: Contam o número de pacotes enviados ou recebidos que são destinados a múltiplos destinos (broadcast) ou a um grupo específico de destinos (multicast). O monitoramento desses contadores pode ajudar a identificar tráfego excessivo ou anomalias.

Além das estatísticas de tráfego, os switches gerenciáveis também fornecem contadores de erros, que são fundamentais para diagnosticar problemas de conectividade física e de transmissão. São contadores de erros comuns em portas de switches:

- **Erros de CRC (*Cyclic Redundancy Check*)**: Indicam quadros de Ethernet corrompidos durante a transmissão, geralmente devido a problemas de integridade do cabo, ruído eletromagnético ou falhas de hardware. Um número elevado de erros de CRC pode sinalizar a necessidade de inspeção ou substituição do cabeamento.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

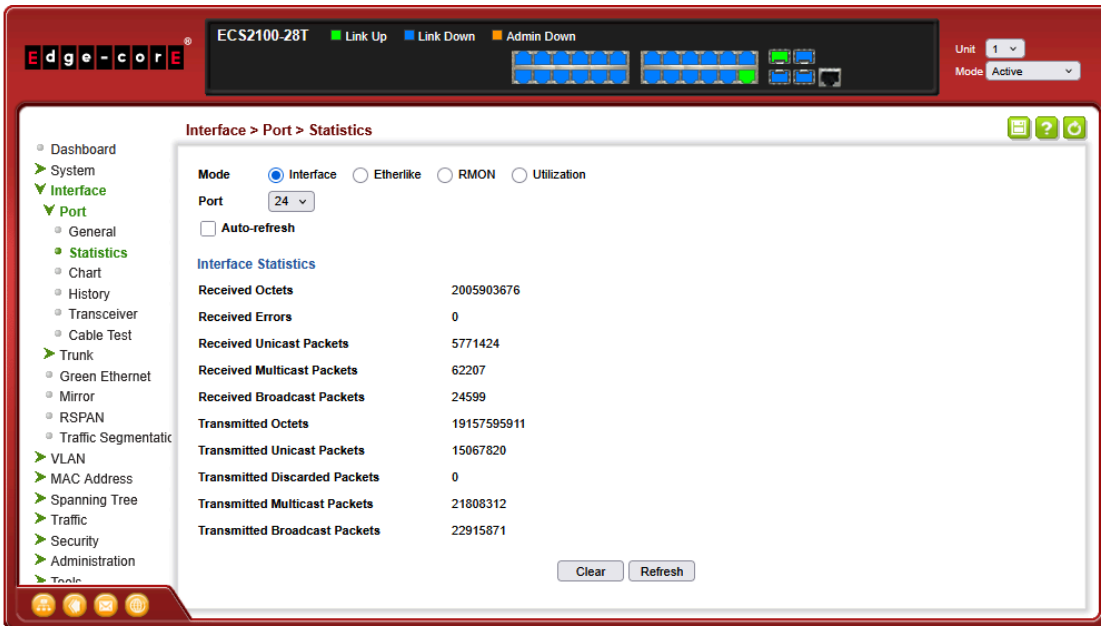
- **Colisões**: Em redes *half-duplex* (raramente utilizadas em implementações modernas, mas ainda presentes em alguns equipamentos legados), este contador indica o número de vezes que dois dispositivos tentaram transmitir simultaneamente. Em redes *full-duplex*, colisões não devem ocorrer.
- ***Late Collisions***: Colisões que ocorrem após o tempo de *slot* normal, geralmente indicando problemas graves na rede física, como cabos excessivamente longos ou problemas de terminação.
- ***Frame Too Long/Too Short***: Contam o número de quadros Ethernet que excederam ou não atingiram o tamanho mínimo ou máximo permitido pelo padrão. Isso pode indicar problemas de configuração ou incompatibilidade entre dispositivos.
- ***Runts/Giants***: Pacotes que são significativamente menores (*runts*) ou maiores (*giants*) do que o tamanho esperado. *Runts* podem ser causados por colisões ou problemas de hardware, enquanto *giants* podem indicar configurações incorretas de MTU (*Maximum Transmission Unit*), por exemplo com a ativação de *jumbo frames*.
- ***Input/Output Errors***: Contadores genéricos que podem indicar diversos problemas na recepção ou transmissão de pacotes, muitas vezes necessitando de uma investigação mais aprofundada.
- ***Discarded Packets***: Número de pacotes que foram descartados pela porta devido a congestionamento, políticas de QoS, violações de segurança ou outros motivos configurados no switch.

Na Tabela 13 estão exemplos da configuração em switches diversos.

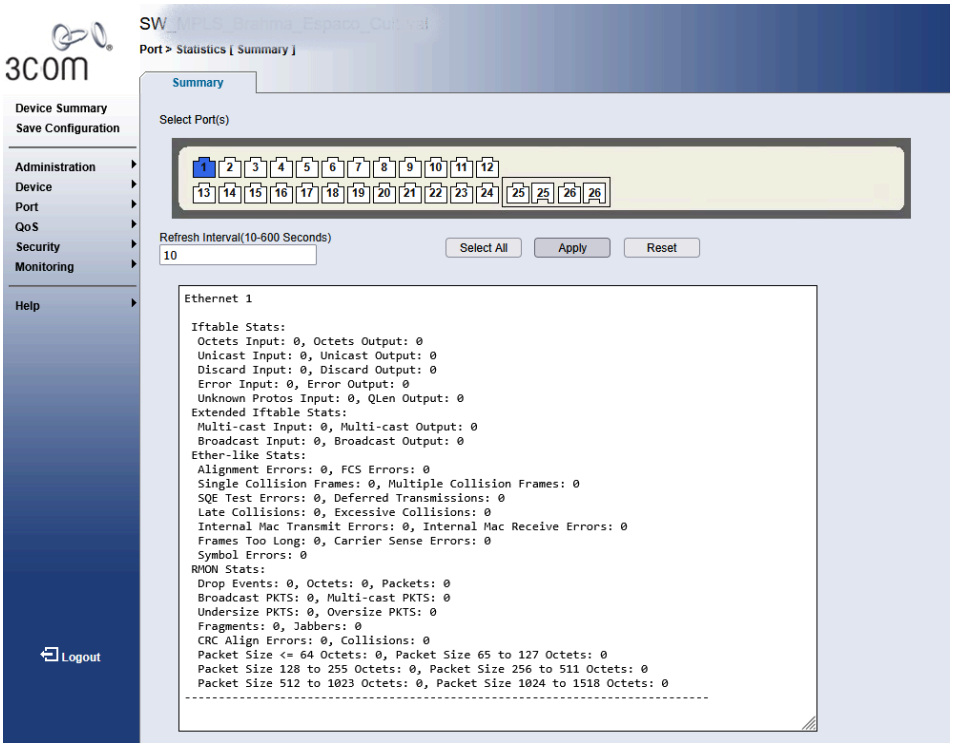
Tabela 13. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch#show int GigabitEthernet1/0/5* *switch# show interfaces status* *switch#show interfaces counters*
Huawei S5720-52X-LI (CLi) *<switch> display interface GigabitEthernet0/0/5* *<switch> display interface brief* *<switch> display counters*
Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



3com 2226 (Web)



3.4 Portas de Fibra Óptica

As portas de fibra óptica são interfaces do tipo SFP que utilizam conversores (*transceivers*) do tipo miniGBIC para conexão de cabos de fibra óptica O uso de fibra óptica

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

possibilita maior largura de banda e, principalmente, maior alcance em comparação com as portas metálicas. Na Figura 25, um exemplo de interface SFP com um conversor miniGBIC para conexão de fibra óptica.

Figura 25. Interface SPF com uso de conversor miniGBIC.

Características

Diferentemente das portas metálicas tradicionais, as portas SFP não possuem um transceptor fixo; em vez disso, aceitam módulos SFP intercambiáveis que determinam o tipo de conexão suportada (fibra monomodo, fibra multimodo ou, em alguns casos, até mesmo cobre). Essa flexibilidade permite que seja personalizado as interfaces do switch de acordo com as necessidades específicas de cada conexão.

Quando utilizadas com módulos de fibra óptica, as portas SFP oferecem diversas vantagens significativas. A principal delas é a capacidade de transmitir dados a distâncias muito maiores do que as permitidas pelos cabos de par trançado de cobre, que geralmente são limitados a 100 metros. As conexões de fibra óptica podem alcançar quilômetros, tornando-as ideais para interconectar switches em diferentes edifícios, conectar a data centers ou estabelecer links de uplink de alta capacidade.

Outra característica importante é a imunidade a interferências eletromagnéticas (EMI) e de radiofrequência (RFI) inerente à transmissão por fibra óptica. Isso garante uma comunicação mais estável e confiável em ambientes eletricamente ruidosos, onde cabos de cobre poderiam sofrer degradação do sinal.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Estatísticas

As estatísticas e contadores das portas metálicas estão disponíveis nas portas tipo SFP. Entretanto, existem informações e estatísticas específicas para SFP que possuem algumas particularidades devido ao uso de conversores de fibra óptica. Algumas das informações que estão disponíveis em switches são:

- **Potência Óptica de Transmissão (*Tx Power*)**: Mede a potência do sinal óptico que o módulo SFP está transmitindo. Este valor é crítico para garantir que o sinal chegue ao dispositivo remoto com intensidade suficiente. Valores fora da faixa esperada podem indicar problemas com o módulo ou a conexão.
- **Potência Óptica de Recepção (*Rx Power*)**: Mede a potência do sinal óptico que o módulo SFP está recebendo. Um sinal muito fraco pode indicar atenuação excessiva na fibra (devido a distância, emendas, ou sujeira nos conectores), problemas no transmissor remoto ou falha no módulo receptor. Um sinal muito forte pode saturar o receptor.
- **Temperatura do Módulo SFP**: Muitos módulos SFP possuem sensores de temperatura internos. Monitorar a temperatura pode ajudar a identificar problemas de superaquecimento que podem levar à falha do módulo.
- **Tensão de Alimentação do Módulo SFP**: Informa a tensão que está sendo fornecida ao módulo. Variações fora da especificação podem indicar problemas de alimentação no switch.
- **Corrente de Polarização do Laser (*Bias Current*)**: Mede a corrente elétrica que alimenta o laser dentro do módulo transmissor. Alterações significativas podem indicar degradação ou falha iminente do laser.
- **Tipo de Módulo SFP e Informações do Fabricante**: O switch geralmente consegue identificar o tipo de módulo SFP inserido (por exemplo, 1000BASE-SX, 10GBASE-LR), o fabricante e o número de série. Isso ajuda a verificar a compatibilidade e a rastrear os componentes.
- **Comprimento de Onda**: Para módulos ópticos, o comprimento de onda da luz utilizada (por exemplo, 850nm, 1310nm, 1550nm) é uma informação importante para garantir a compatibilidade com a fibra e outros equipamentos.

Na Tabela 14 estão exemplos da configuração em switches diversos.

Tabela 14. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)
switch>enable

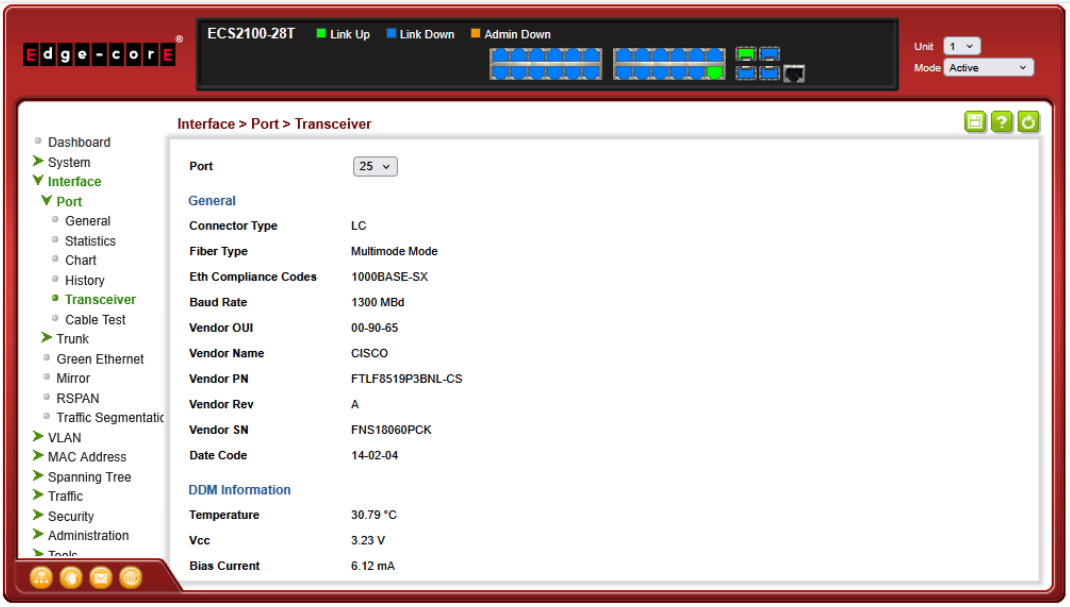
Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

switch#show interfaces transceiver detail

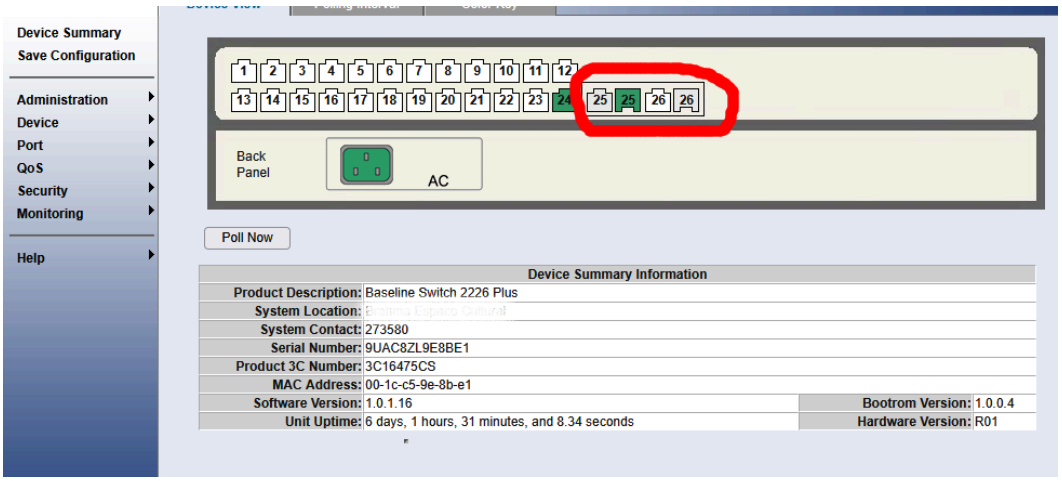
Huawei S5720-52X-LI (CLi)

<switch> display transceiver interface XGigabitEthernet0/0/1 verbose

Edgecore ECS2100-28T (Web)



3com 2226 (Web)



** Este switch não possui estatísticas específicas para conexão com conversores de fibra. Outra característica é o compartilhamento de portas entre a porta metálica e a porta para o SFP (portas 25 e 26), sendo somente uma das conexões permitidas por vez.*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

3.5 Agente SNMP

O agente do protocolo SNMP (*Simple Network Management Protocol*) é um serviço executado no sistema operacional do switch para prover gerenciamento. O agente mantém um banco de dados local, conhecido como MIB (*Management Information Base*), que organiza todas as métricas e configurações gerenciáveis do switch em uma estrutura hierárquica. O serviço permite o gerenciamento e o monitoramento remoto do switch por meio de um software de gerenciamento de rede (NMS). O agente coleta informações sobre o dispositivo e responde a requisições do NMS por meio de pacotes SNMP. O protocolo SNMP utiliza na camada de transporte o protocolo UDP na porta 161 por padrão. Em caso de uso de Traps, que são mensagens SNMP originadas do agente para o gerente, a porta utilizada é a UDP 162.

Introdução ao protocolo SNMP - https://youtu.be/q4B6NOmFDNA

A configuração é realizada com a ativação do agente, definição da versão do protocolo (v1, v2c ou v3), definição da comunidade (*community*), por padrão é "public" somente leitura e "private" para leitura e escrita, e em alguns casos o IP do gerente SNMP deve ser configurado. A versão do protocolo mais comum é a 2c, que embora não possua recursos mais avançados de segurança como a versão 3, ainda é muito utilizada. Na Tabela 15 estão exemplos da configuração em switches diversos.

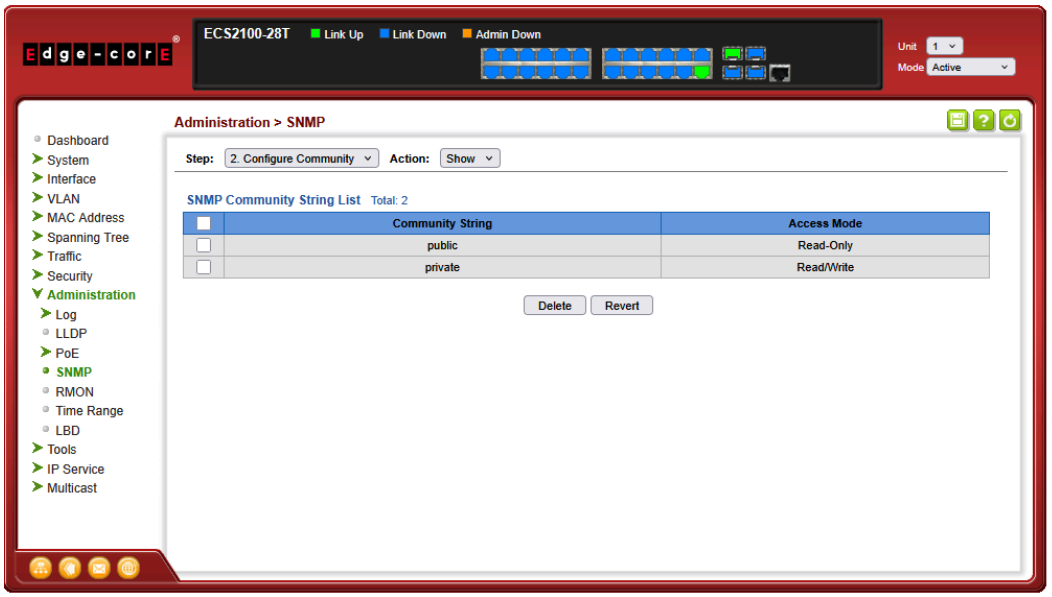
Tabela 15. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch#conf t* *switch(config)# snmp-server community public ro* *switch(config)# snmp-server location Rack13* ** Agente SNMP na versão 2c*
Huawei S5720-52X-LI (CLi) *<switch> system-view* *[switch] snmp-agent community complexity-check disable* *[switch] snmp-agent* *[switch] snmp-agent sys-info version v2c* *[switch] snmp-agent community read cipher* ***public*** *mib-view View_ALL*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

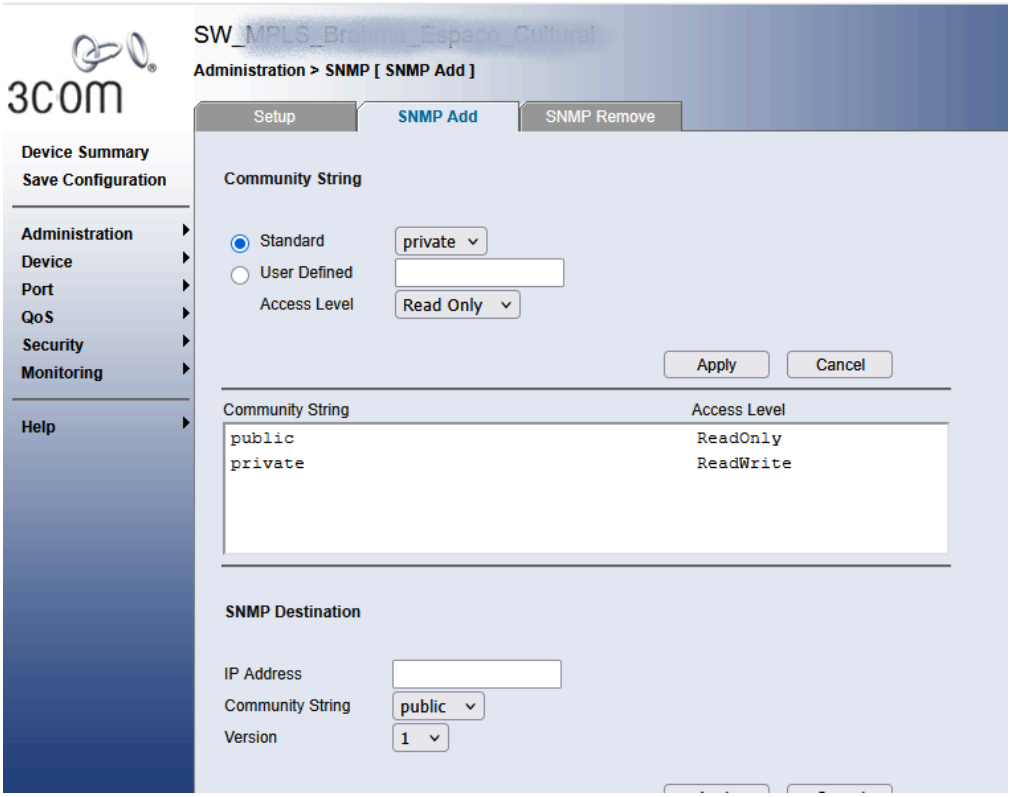
*Agente SNMP na versão 2c; o comando “snmp-agent community complexity-check disable” desabilita a checagem da complexidade do nome da comunidade para permitir o uso de “public”

Edgecore ECS2100-28T (Web)



3com 2226 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



3.6 Logs

Os logs são registros cronológicos de eventos que ocorrem no switch, como erros, mudanças de estado das interfaces, atividades de segurança e ações administrativas. São fundamentais para o diagnóstico de problemas e a auditoria da rede. O formato do logs poderá variar entre modelos diferentes de switches, desta forma devem ser adaptadas às ferramentas de análise para cada tipo de log.

Administração de Logs - https://www.youtube.com/watch?v=_0kxboqXfIY

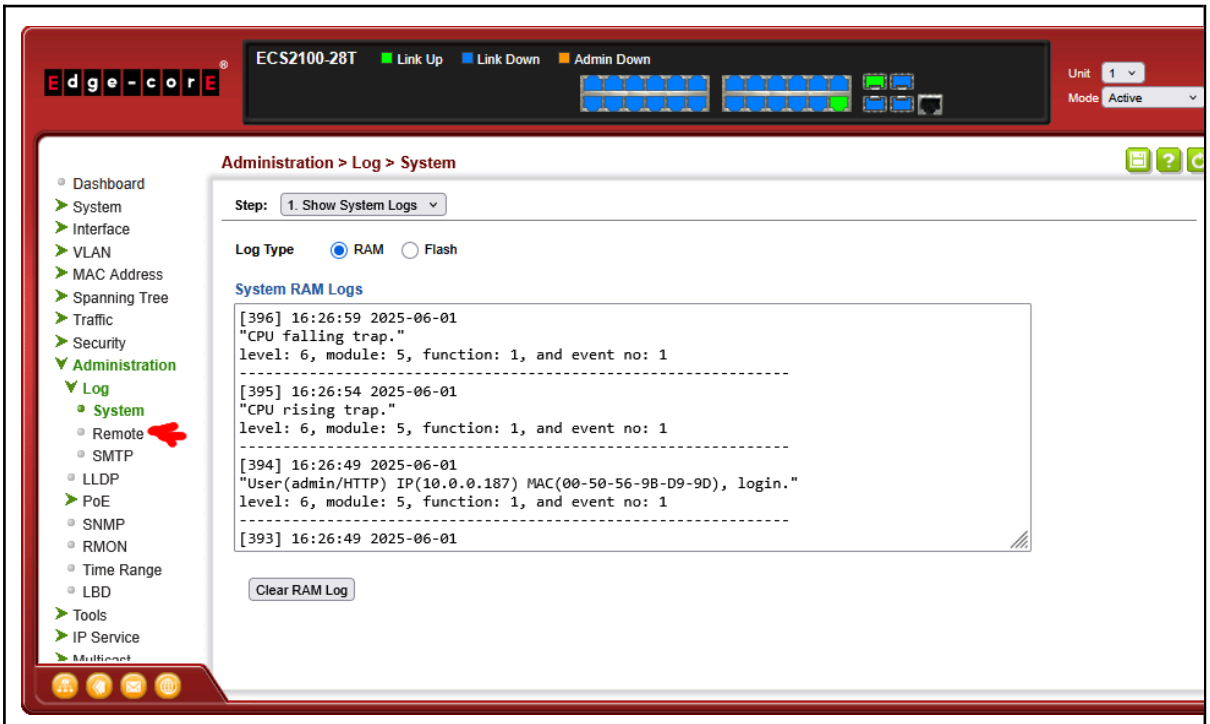
O espaço para armazenamento nos switches é bastante reduzido e isto permite um número bastante limitado de logs disponibilizados. Outro fator importante a observar é a inexistência de armazenamento persistente de logs no switches. Portanto, em caso de um desligamento serão perdidos os logs. Para evitar esta perda deve ser ativado um servidor de logs (*remote syslog server*) para receber os logs dos switches e poder realizar análises de anomalias e histórico de eventos. O servidor de logs remoto deverá ser alcançável pelo switch, por exemplo, estar na mesma VLAN de gerenciamento. Na Tabela 16 estão exemplos da configuração em switches diversos.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

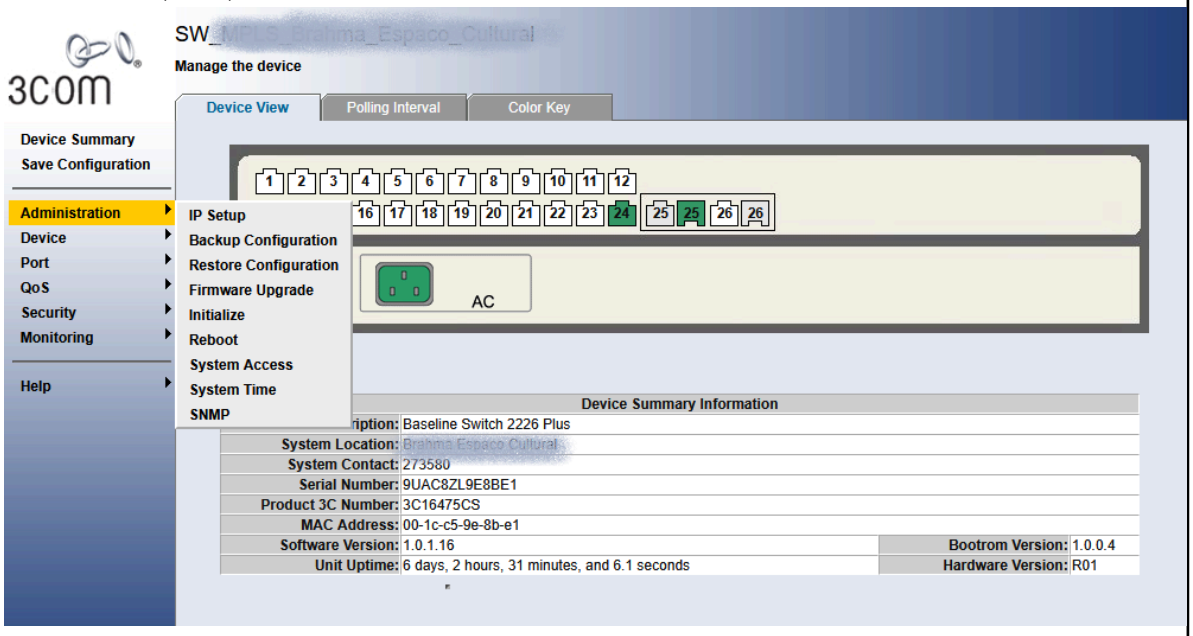
Tabela 16. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch# show loggging* *switch#conf t* *switch(config)# logging on* *switch(config)#logging **10.0.0.22*** **O endereço IP 10.0.0.22 é do servidor de logs remoto* *switch(config)# logging trap **errors*** **Para escolher o nível de log a ser enviado para o servidor remoto, são estes os níveis disponíveis:* *emergencies* *alerts* *critical* *errors* *warnings* *notifications* *informational (default level)* *debugging*
Huawei S5720-52X-LI (CLi) *<switch> display logbuffer* *<switch> system-view* *[switch] info-center enable* *[switch] info-center loghost **10.0.0.22** port 514* *[switch] info-center channel loghost log level debugging* *[switch] info-center loghost source Vlanif1* ** O comando " info-center loghost source Vlanif1" configura em qual interface virtual disponível no switch serão enviados os logs para o servidor (normalmente será a interface virtual que pertence a VLAN de gerenciamento)*
Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional



3com 2226 (Web)



** Este modelo não possui funcionalidades de logs locais e nem possibilidade de envio de logs para um servidor remoto.*

3.7 Tabela MAC

A tabela de endereços MAC (*Media Access Control*), também conhecida como tabela CAM (*Content Addressable Memory*), é o núcleo do processo de encaminhamento de tráfego

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

em um switch. A partir das trocas de pacotes, o switch aprende a localização dos dispositivos nas portas, construindo uma tabela dinâmica atualizada de endereços MAC. O comportamento é similar a um banco de dados mantido pelo switch que associa endereços MAC de dispositivos conectados às suas respectivas portas e VLANs.

Por meio da tabela MAC é possível identificar a localização de dispositivos pelo endereço da interface, validar se um determinado MAC está na VLAN correta e se existem dispositivos conectados em um portas e quantos são. Normalmente, será disponibilizada uma forma de realizar buscas por endereços MAC na tabela CAM. O formato do endereço MAC não é padrão entre os fabricantes, alguns utilizam o separado com ":", outros com "-" ou ".". Os campos podem ser agrupados de forma distinta, usando por byte ou por pares de bytes, por exemplo, 21:10:AB:90:2C:01, 21-10-AB-90-2C-01, 2110-AB90-2C01 e 2110.AB90.2C01.

A quantidade de endereços MAC que podem ser armazenados por um switch depende dos recursos de memória e de processamento disponíveis. Por exemplo, em switches de entrada, com baixos recursos computacionais, o tamanho máximo da tabela MAC é de 8.000 endereços. Em casos onde o switch não possui um endereço aprendido na tabela MAC, o pacote será enviado para todas as portas ativas. Este processo é normal na inicialização do switch ou na conexão de um novo dispositivo na rede. Entretanto, existem ataques tais como **MAC *Flooding*** e **MAC *Spoofing*** que podem ser mitigados ativando proteções disponíveis em alguns switches. Estes ataques possuem estas características:

- **MAC *Flooding***: o ataque de MAC flooding é gerado por um grande número de endereços MAC de origem falsificados que são enviados ao switch para sobrecarregar a tabela CAM. Ao atingir a capacidade máxima, o switch pode começar a se comportar como um hub, inundando o tráfego para todas as portas, comprometendo a segurança e o desempenho.
- **MAC *Spoofing***: Alguns switches podem detectar situações onde um dispositivo tenta usar o endereço MAC de outro dispositivo já conhecido na rede (MAC spoofing), e tomar ações para prevenir a comunicação fraudulenta.

Estas proteções, quando disponíveis no switch, devem ser ativadas para evitar incidentes. Na Tabela 17 estão exemplos da configuração em switches diversos.

Tabela 17. Exemplos da configuração em switches diversos.

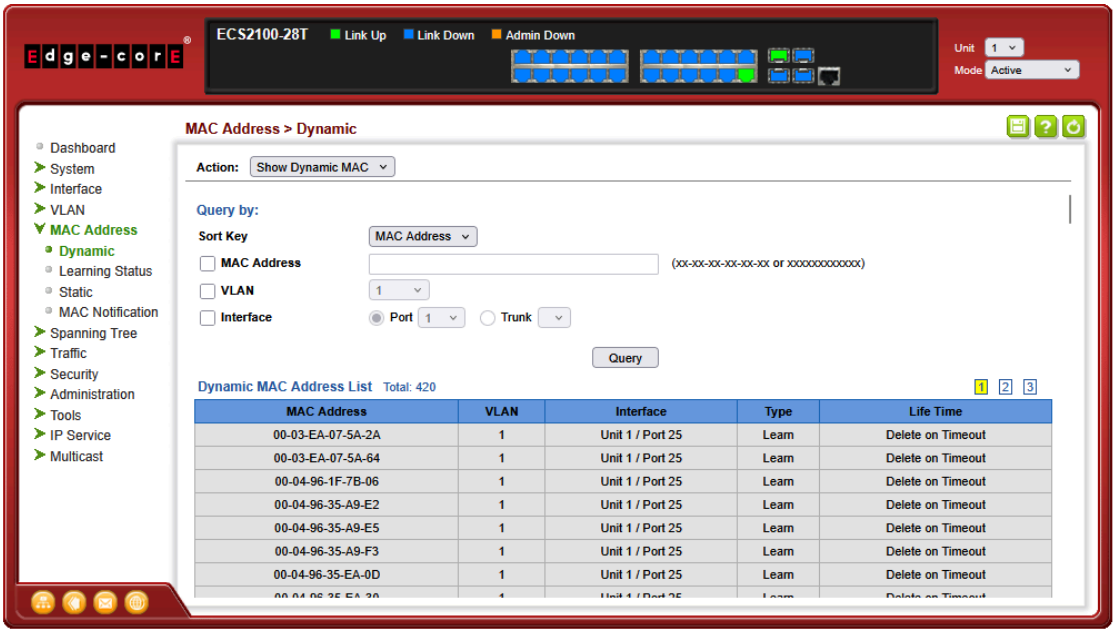
Cisco 2960 (CLI)
switch>enable *switch#show mac address-table* *switch#show mac address-table interface gigabitEthernet 1/0/8* *switch#show mac address-table address ac8b.a954.b7df*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

Huawei S5720-52X-LI (CLi)

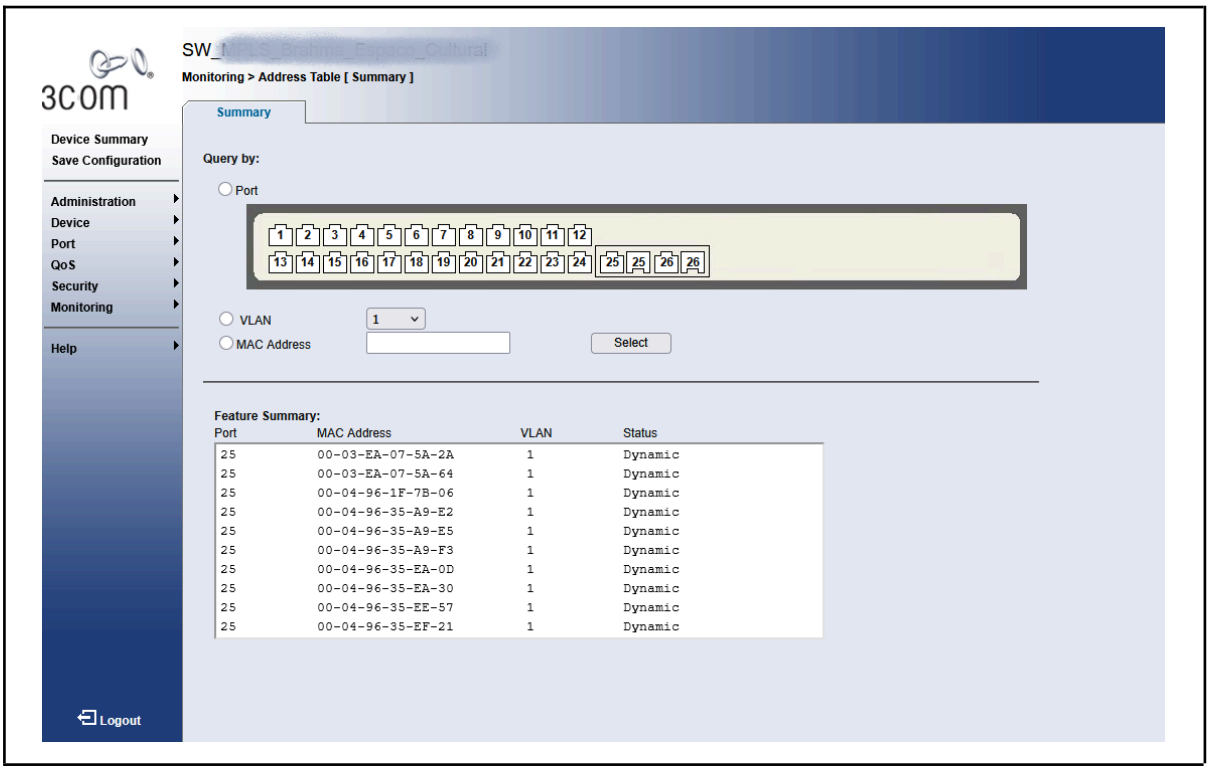
<switch> display mac-address
<switch> display mac-address g0/0/8
<switch> display mac-address ac8b-a954-b7df

Edgecore ECS2100-28T (Web)



3com 2226 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



3.8 LLDP (Link Layer Discovery Protocol)

O LLDP (*Link Layer Discovery Protocol*), padronizado como IEEE 802.1AB, é um protocolo de descoberta de vizinhança que permite que dispositivos de rede anunciem suas informações de identidade e capacidades para outros dispositivos diretamente conectados na mesma rede local. O protocolo de camada de enlace utiliza comunicação em multicast, que permite que dispositivos de rede vizinhos anunciem suas informações de identidade e capacidades uns aos outros, facilitando o mapeamento da topologia da rede.

Protocolo LLDP: Dica de uso - https://youtu.be/B47owGIwBE0

Esta funcionalidade permite que sejam identificados dispositivos conectados nas portas do switch tais como telefone VOIP, *access points*, roteadores e qualquer dispositivo que tenha o serviço LLDP ativo. O serviço não deve ser ativado em portas de usuários (*edge ports*) que não utilizem LLDP. O motivo é devido às informações que são enviadas nos pacotes do LLDP conter endereço IP de gerenciamento, versão do firmware, modelo do dispositivo entre outros que não precisam ser públicos. Na Tabela 18 estão exemplos da configuração em switches diversos.

Tabela 18. Exemplos da configuração em switches diversos.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

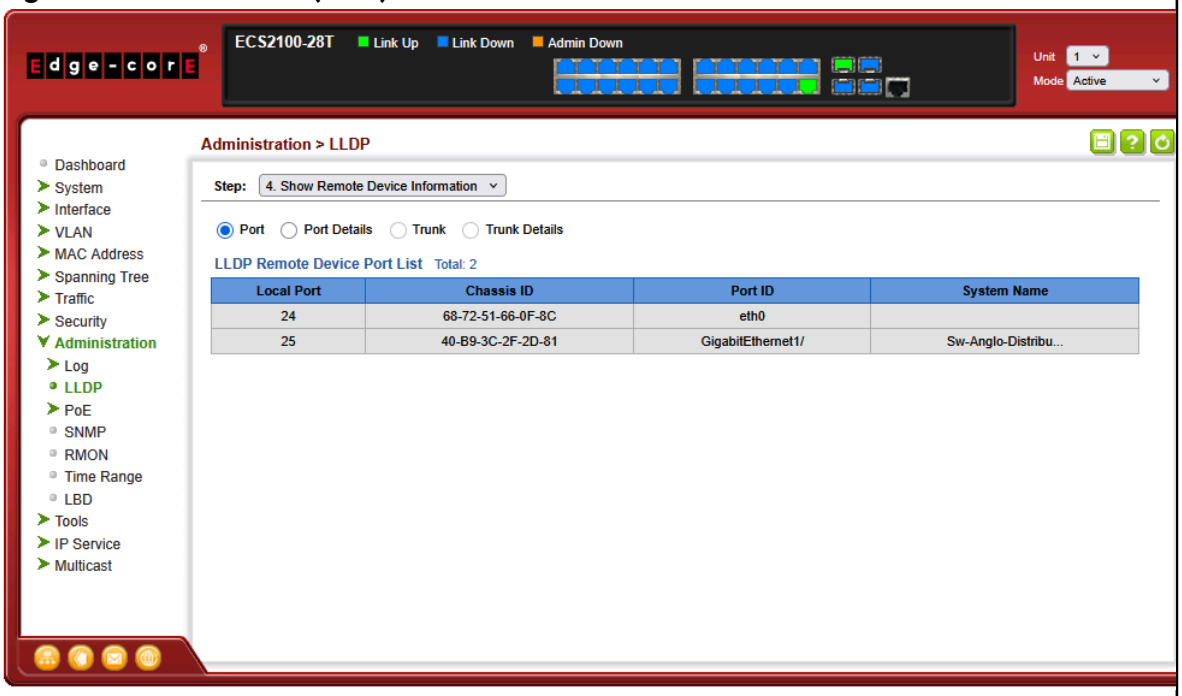
Cisco 2960 (CLI)

switch>enable
switch#conf t
switch(config)# lldp run
switch# show lldp neighbors

Huawei S5720-52X-LI (CLi)

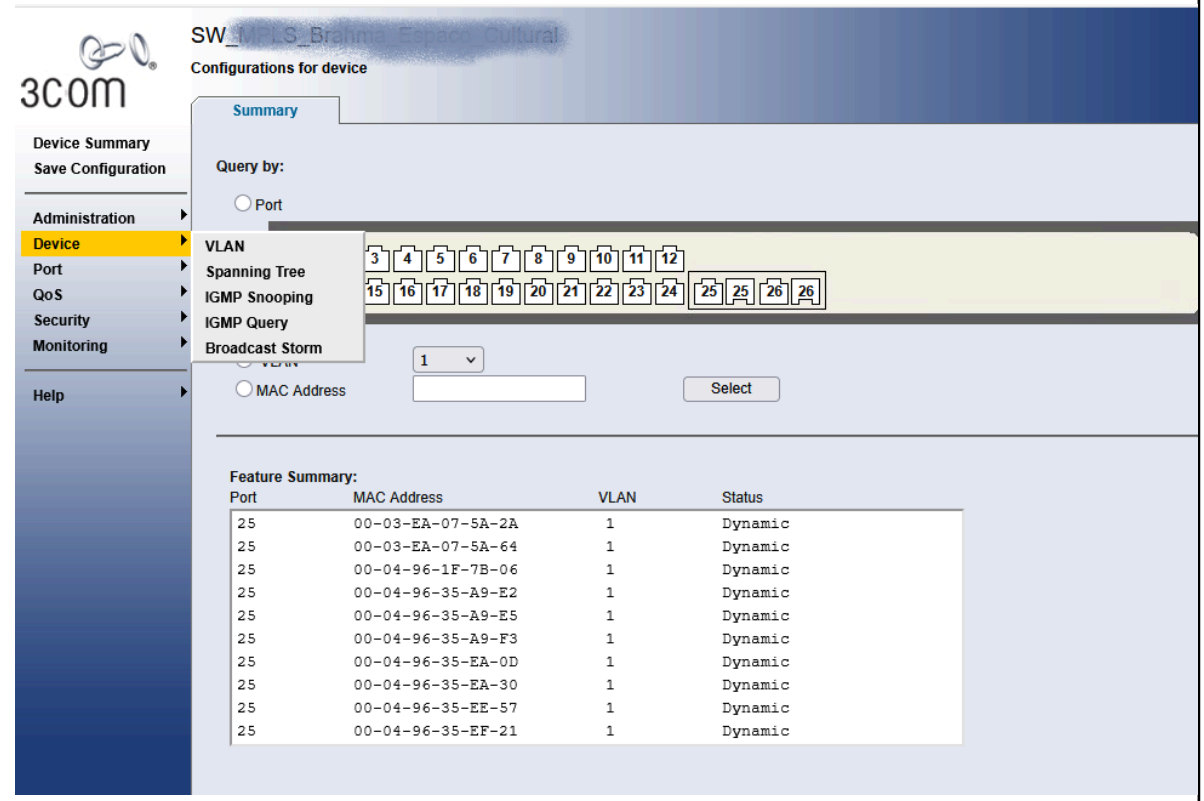
<switch>system-view
[switch] lldp enable
<switch> display lldp neighbor

Edgecore ECS2100-28T (Web)



3com 2226 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



** Este modelo não possui funcionalidades de LLDP.*

3.9 Controles de Tráfego Broadcast e Multicast

Os controles de tráfego são mecanismos para limitar a propagação de tráfego broadcast (destinado a todos os dispositivos na rede) e multicast (destinado a um grupo específico de dispositivos), evitando a sobrecarga da rede e otimizando a largura de banda. Estes controles são aplicados por interface de rede no switch e são configurados em número de pacotes por segundo ou pela largura de banda máxima que poderá ser usada para pacotes em broadcast ou multicast. Em caso do tráfego exceder o limite, os pacotes serão descartados pelo switch.

Combatendo loops na rede - https://www.youtube.com/watch?v=aprt2k4dVEE

Em uma rede com comportamento normal, uma interface de rede do switch conectada em um dispositivo, tal como um desktop ou uma impressora, gera dezenas de pacotes por segundo em broadcast ou multicast. Estes pacotes são usados por protocolos de descoberta, tais como DHCP, SSDP, mDNS, que tem como princípio de funcionamento o envio de pacotes de forma periódica. Deve-se observar que o uso de transmissões em

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

multicast de áudio ou vídeo geram milhares de pacotes por segundo e serão bloqueadas nas interfaces que estiverem com restrições de controles de tráfego multicast. O protocolo IPv6 faz uso de transmissões em multicast para descoberta de vizinhos e de *gateways*. Entretanto, a quantidade de pacotes por segundo nestes casos será muito abaixo, por exemplo, do que é gerado por um loop físico na rede.

Em situações de *loop* de camada 2, a proliferação de pacotes pode escalar rapidamente para milhões por segundo, levando ao congestionamento da rede e, potencialmente, ao travamento do switch. Portanto, configura-se como uma prática recomendada a implementação de limites na taxa de pacotes ou na largura de banda consumida por tráfego *broadcast* e *multicast* em interfaces conectadas a dispositivos de usuários finais. Para interfaces de *uplink*, que agregam tráfego de múltiplas fontes e podem transportar tráfego *broadcast* e *multicast* legítimo de serviços como DHCP, é aconselhável definir limites superiores de taxa de pacotes e largura de banda máxima que não prejudique a comunicação com os serviços. Na Tabela 19 estão exemplos da configuração em switches diversos.

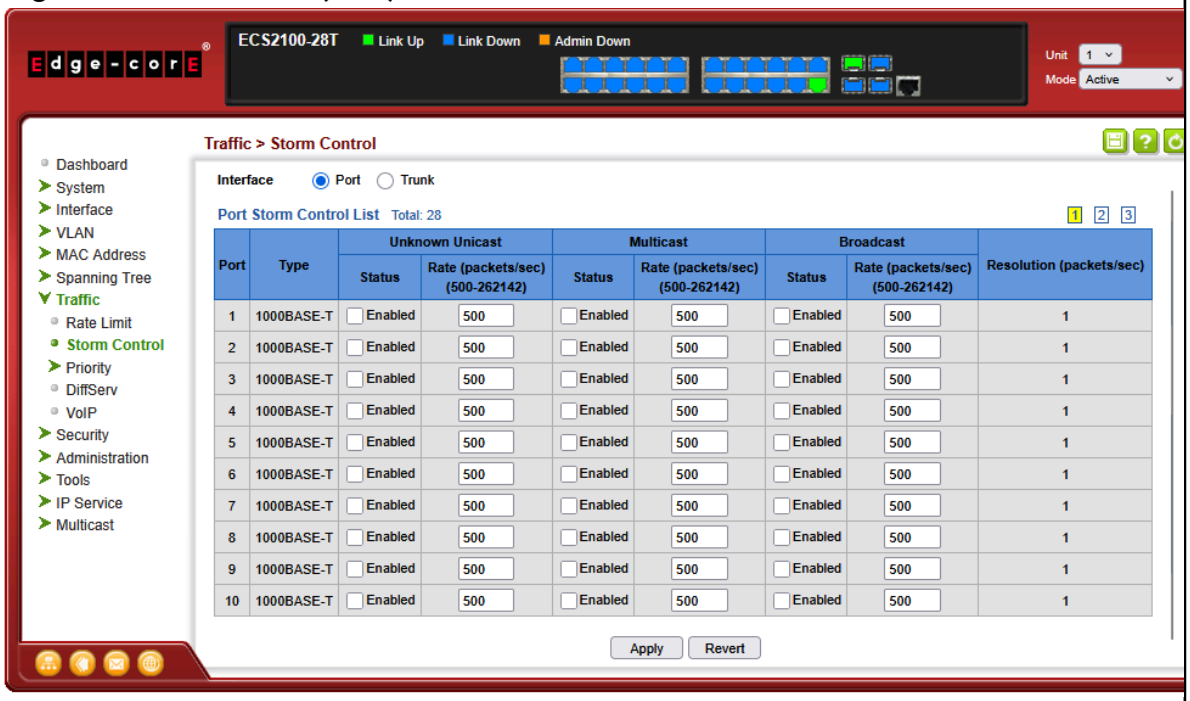
Tabela 19. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch#conf t* *switch(config)# interface fastEthernet 0/1* *switch(config-if)#storm-control broadcast level 10* *switch(config-if)#storm-control multicast level 10* ***ou*** *switch(config-if)#storm-control broadcast level pps 50* *switch(config-if)#storm-control multicast level pps 50* ** O nível (level) define a porcentagem da largura de banda na qual pacotes em broadcast podem ocupar, no intervalo de 1s. No exemplo, no máximo, 10% dos pacotes na interface f0/1 poderão ser em broadcast, no intervalo de 1s. Acima deste limite, os pacotes serão bloqueados (padrão). A diretiva pps significa packets per second (pacotes por segundo).*
Huawei S5720-52X-LI (CLi) *<switch> system-view* *[switch] int GigabitEthernet 0/0/1* *[switch-GigabitEthernet0/0/1] broadcast-suppression percent 10* *[switch-GigabitEthernet0/0/1] multicast-suppression percent 10* ***ou*** *[switch-GigabitEthernet0/0/1] broadcast-suppression packets 50* *[switch-GigabitEthernet0/0/1] multicast-suppression packets 50*

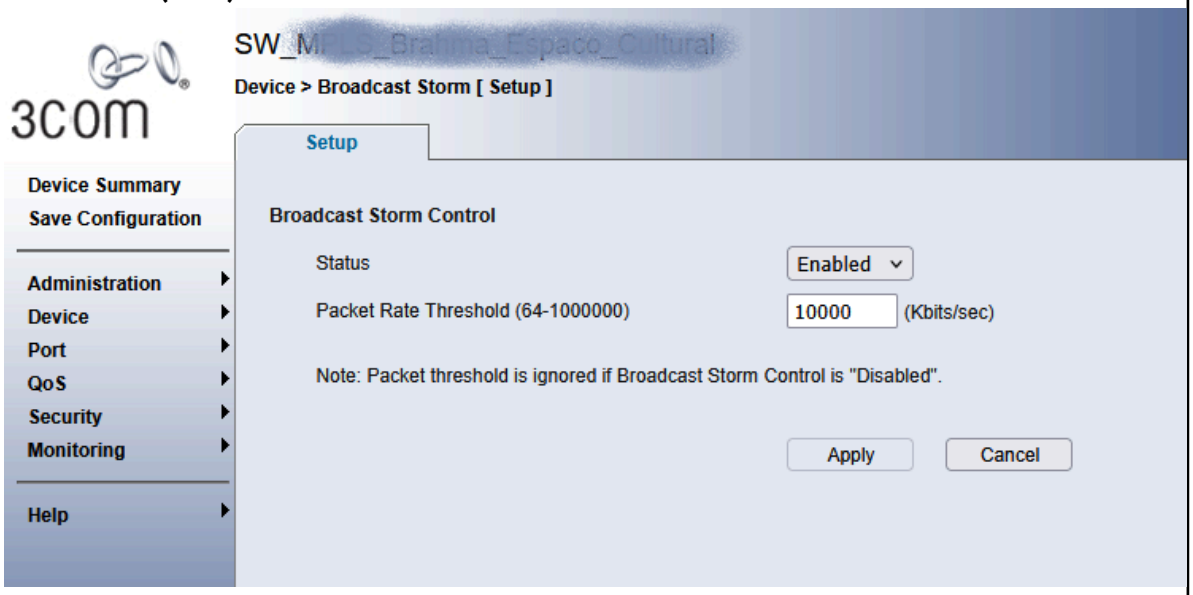
Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

*O comando “broadcast-suppression percent 10” limita em 10% os pacotes broadcast na interface. O comando “broadcast-suppression packets 50” limita em 50 pacotes de broadcast por segundo na interface.

Edgecore ECS2100-28T (Web)



3com 2226 (Web)



* Neste modelo existe apenas uma opção de limitação que afeta todas as portas do switch.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

3.10 Salvar a configuração

O salvamento das configurações tem como objetivo armazenar configurações atuais de uma forma persistente. Ao aplicar as configurações e realizar procedimentos nos switches o efeito será imediato em grande parte das ações, por exemplo como modificações em VLANs ou alterações em velocidades de interfaces. Alguns procedimentos, por exemplo o *upload* de um novo *firmware*, só será ativado no próximo reboot do equipamento. Para salvar as configurações atuais, em execução, deve-se executar a funcionalidade de salvar configurações.

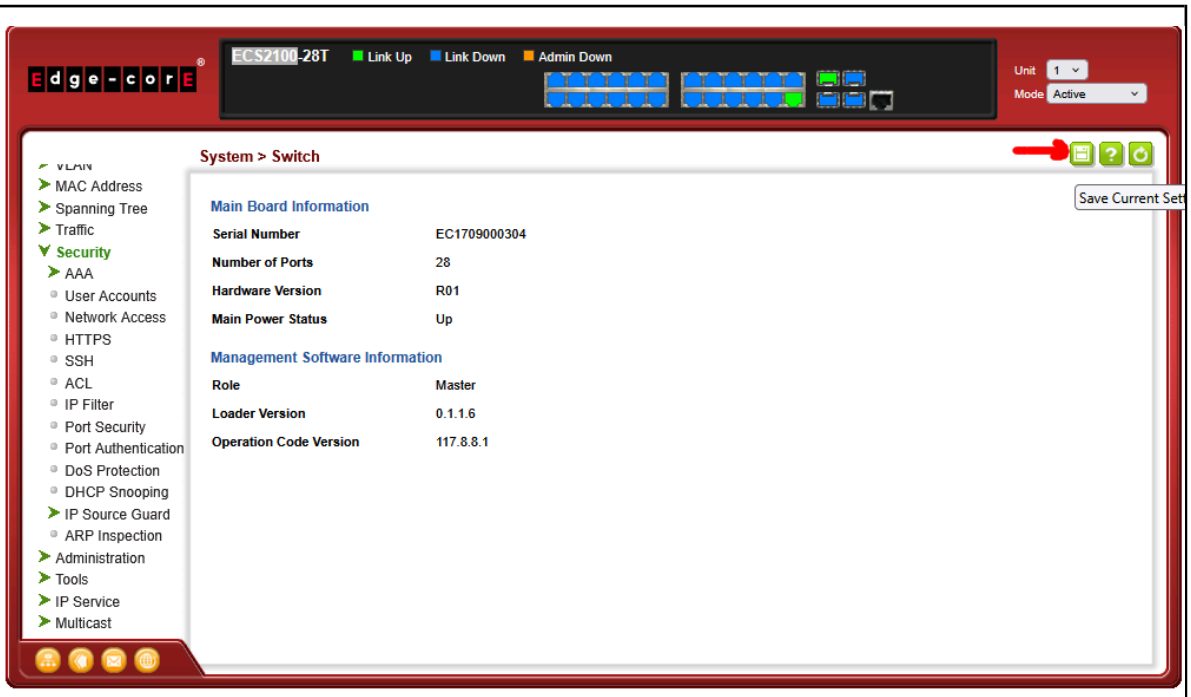
Caso não seja realizado o salvamento da configuração, no próximo reboot estas serão perdidas. Por mais lógico que possa parecer, salvar as configurações é por vezes esquecido pelo administrador de rede. O efeito será posterior, na próxima reinicialização do equipamento haverá uma surpresa desagradável. Portanto, é uma boa prática realizar o salvamento da configuração atual assim que estiver funcional.

Em algumas ocasiões, o não salvamento da configuração pode ser proposital. Por exemplo, durante a avaliação de uma nova configuração em um ambiente de produção, a não realização do salvamento oferece um mecanismo de *rollback* simplificado. Uma reinicialização do switch reverterá o equipamento para o estado configurado previamente. Essa abordagem é particularmente vantajosa em cenários de acesso remoto ao dispositivo, onde solicitar a uma pessoa não técnica um procedimento de desligar e ligar um switch pode ser mais prático do que instruir esta pessoa a executar comandos complexos na interface de configuração. Na Tabela 20 estão exemplos da configuração em switches diversos.

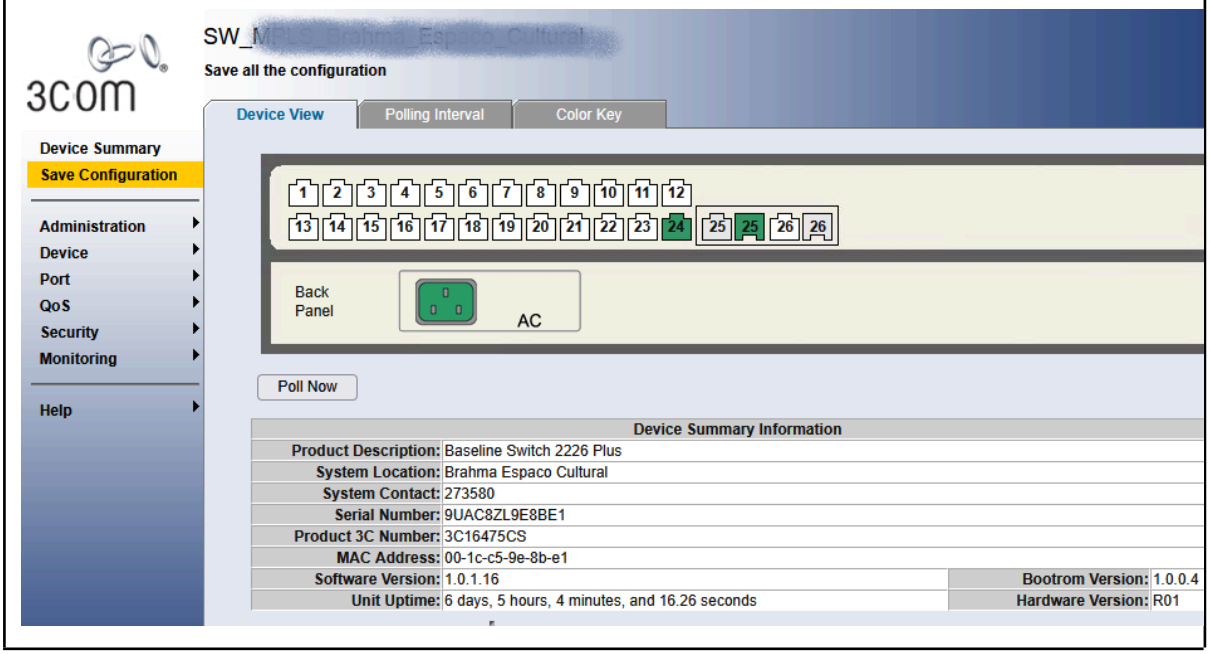
Tabela 20. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch#copy running-config startup-config* ***ou*** *switch#wr*
Huawei S5720-52X-LI (CLi) *<switch> save*
Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



3com 2226 (Web)



3.11 Backup/Restore

O Backup e o Restore são funcionalidades que permitem salvar a configuração atual do switch em um arquivo (backup), armazená-lo em outro local e restaurá-la posteriormente, facilitando a recuperação em caso de falhas ou erros de configuração.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

A frequência dos backups deve ser determinada pela criticidade da rede e pela frequência de alterações na configuração. Ambientes dinâmicos com mudanças frequentes exigem backups mais regulares. Recomenda-se realizar um backup antes de qualquer alteração significativa na configuração, atualização de *firmware* ou intervenção de manutenção no equipamento. Em alguns switches é possível gerar um arquivo de backup no próprio switch, o que facilita o restore em caso de necessidade.

Os switches gerenciáveis geralmente oferecem múltiplos métodos para realizar o backup das configurações:

- **Interface de Linha de Comando (CLI):** Utilização de comandos específicos para exportar a configuração para um arquivo de texto. Este método oferece flexibilidade e controle granular sobre o processo.
- **Interface Gráfica do Usuário (GUI):** Uma interface web que permite iniciar o processo de backup e especificar o destino do arquivo com uso de um navegador.
- **Protocolos de Transferência de Arquivos:** Suporte a protocolos como TFTP (*Trivial File Transfer Protocol*), FTP (*File Transfer Protocol*) ou SFTP (*SSH File Transfer Protocol*) para transferir o arquivo de configuração para um servidor de backup centralizado. Estes protocolos permitem que seja feito o backup e o resto de forma remota e automatizada. Na Figura 26, está um exemplo do uso de um servidor de TFTP usado para o download da configuração atual em um switch Cisco modelo 2960.

Protocolo TFTP - https://youtu.be/bs_6uW_d9Yc

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

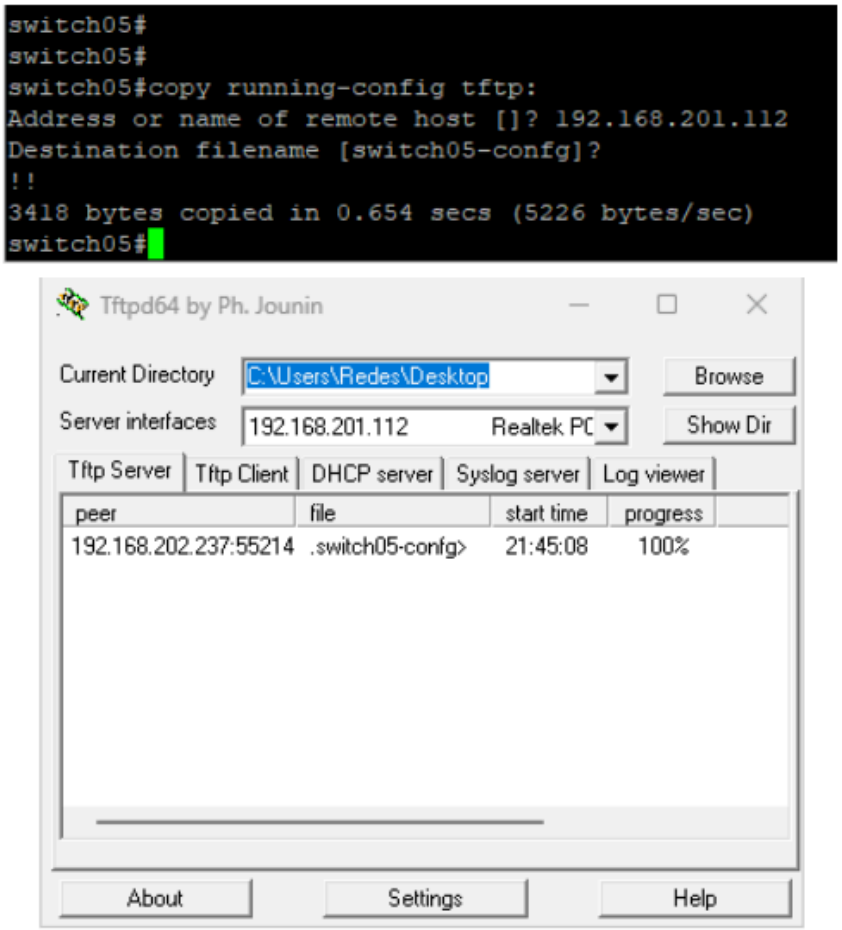


Figura 26. Uso de um servidor TFTP para o download da configuração em um switch Cisco modelo 2960.

O processo de restauração (*restore*) envolve a aplicação de um arquivo de configuração previamente salvo ao switch. Esta operação pode ser necessária nas seguintes situações:

- **Substituição de Hardware:** Em caso de falha irreparável do switch, a restauração da configuração em um novo equipamento minimiza o tempo de inatividade e acelera a recuperação da rede. Nestes casos, o switch substituto deverá ser compatível com a configuração do backup, do mesmo modelo e na mesma versão do firmware.
- **Reversão de Configurações:** Se uma nova configuração introduzir problemas ou instabilidade na rede, a restauração de um backup anterior permite um retorno rápido a um estado operacional conhecido e confiável.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Recuperação de Erros de Configuração:** Em situações onde configurações incorretas foram aplicadas, a restauração de um backup limpo pode ser mais eficiente do que a identificação e correção manual de múltiplos erros.

Os arquivos de backup deverão ser mantidos em um ambiente seguro e de forma organizada, com nomes que identifiquem a data, a versão do modelo do switch e o firmware no qual a configuração foi originada. Na Tabela 21 estão exemplos da configuração em switches diversos.

Tabela 21. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) ***Backup*** *switch>enable* *switch#show running-config* ** Copiar a saída para um texto sem formatação.* ***ou*** *switch# copy startup-config tftp:* ** Apontar para um servidor de TFTP e o nome do arquivo de backup* ***Restore*** *switch# copy tftp: startup-config* ** Apontar para um servidor de TFTP e o nome do arquivo de backup*
Huawei S5720-52X-LI (CLi) ***Backup*** *<switch> display current-configuration* ** Copiar a saída para um texto sem formatação.* **ou** *<switch> display startup* ** Para verificar qual o arquivo que está sendo usado para salvar as configurações.* *<switch> tftp 10.0.0.22 put flash:/vrpcfg.zip S5720-Core-20250601.zip* ** Envia o arquivo atual de configuração para o servidor de TFTP 10.0.0.22 sendo o arquivo final renomeado para S5720-Core-20250601.zip* ***Restore*** *<switch> tftp 10.0.0.22 get S5720-Core-20250601.zip flash:/vrpcfg.zip* ** Copia o arquivo S5720-Core-20250601.zip via servidor de TFTP 10.0.0.22 e armazena com o nome de vrpcfg.zip*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Edgecore ECS2100-28T (Web)

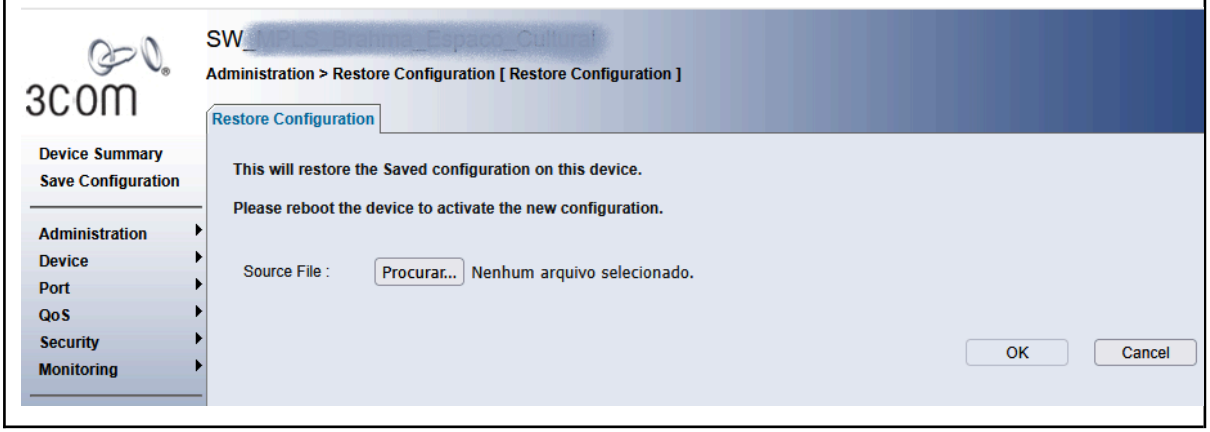
Backup
Vty-1#show running-config
ou
Vty-1#copy startup-config tftp

** Este modelo, no firmware utilizado, não possui as funcionalidades de backup da configuração pela console web. Para realizar este procedimento é possível o acesso pela console em linha de comando por meio de Telnet.*

Restore
Vty-1#copy tftp startup-config

3com 2226 (Web)
Backup

Restore



3.12 Atualização de Software (*Firmware*)

A atualização de software (*firmware*) consiste no processo de substituição da versão atual do sistema operacional do switch por uma versão mais recente, que pode conter novas

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

funcionalidades, correções de *bugs* e melhorias de segurança. Esta atualização possui importantes aspectos que são:

- **Correção de *Bugs*:** Novas versões de *firmware* frequentemente resolvem problemas e falhas de software identificadas em versões anteriores, melhorando a estabilidade e a confiabilidade.
- **Novos Recursos e Funcionalidades:** As atualizações podem introduzir novos protocolos, funcionalidades de gerenciamento, opções de segurança e melhorias no desempenho geral.
- **Otimização de Desempenho:** Fabricantes continuamente otimizam o código do *firmware* para melhorar a velocidade de processamento de pacotes, reduzir a latência e aumentar a capacidade de comutação do switch.
- **Mitigação de Vulnerabilidades de Segurança:** Falhas de segurança descobertas no *firmware* podem ser exploradas por atacantes. As atualizações geralmente incluem *patches* de segurança para proteger o switch contra ameaças.
- **Compatibilidade:** A atualização do *firmware* pode ser necessária para garantir a compatibilidade com novos dispositivos, protocolos de rede ou padrões da indústria.

O processo de atualização de *firmware* varia dependendo do fabricante e do modelo do switch, mas geralmente envolve os seguintes passos:

1. **Verificação da Versão Atual:** Antes de iniciar a atualização, é importante verificar a versão de *firmware* atualmente instalada no switch. Esta informação geralmente pode ser encontrada na interface de gerenciamento (CLI ou GUI).
2. **Download do Novo Firmware:** Acessar o site de suporte do fabricante do switch e localizar a versão de *firmware* mais recente para o seu modelo específico. É muito importante garantir que a versão é a correta para o modelo do hardware. É comum haver revisões de hardware do mesmo modelo de switch e os firmwares não serem compatíveis.
3. **Leitura da Documentação:** Revisar atentamente as notas de lançamento e as instruções de atualização fornecidas pelo fabricante. Estas informações contêm detalhes importantes sobre o processo, possíveis riscos e recomendações.
4. **Backup da Configuração:** Antes de qualquer atualização, é importante realizar um backup completo da configuração atual do switch. Isso permite restaurar o dispositivo para um estado funcional conhecido em caso de falha durante o processo de atualização.
5. **Transferência do Firmware para o Switch:** O arquivo de *firmware* baixado precisa ser transferido para o switch. Isso pode ser feito através de diferentes métodos, como:

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **TFTP (*Trivial File Transfer Protocol*):** Um protocolo simples para transferir arquivos entre um servidor TFTP e o cliente disponível no switch.
- **FTP (*File Transfer Protocol*) ou SFTP (*SSH File Transfer Protocol*):** Protocolos mais seguros para transferência de arquivos.
- **HTTP/HTTPS:** Transferência via navegador web, especialmente para interfaces gráficas.
- **USB:** Alguns switches possuem portas USB para carregar o arquivo de *firmware* diretamente de um dispositivo de armazenamento. O arquivo do firmware deve possuir um nome específico e ao inserir um pendrive na porta USB do switch será feito o processo de instalação.

6. **Início do Processo de Atualização:** O processo de atualização do *firmware* é iniciado através da interface de linha de comando (CLI) ou da interface gráfica web (GUI), dependendo do modelo e da configuração do switch. A documentação fornecida pelo fabricante é um recurso essencial e deve ser consultada minuciosamente para garantir a aplicação correta das instruções específicas para o modelo do equipamento. Durante a execução da atualização, é crítico manter a alimentação de energia estável e não interromper o processo sob nenhuma circunstância. Uma interrupção pode corromper o *firmware*, resultando em danos severos ao switch, tornando-o inoperante.

   A perda de acesso ao dispositivo durante uma atualização de *firmware* ou a aplicação de uma versão incompatível, para a qual não há procedimento de recuperação documentado, leva a um estado conhecido como "***bricking***". Este termo, derivado da palavra inglesa "*brick*" (tijolo), ilustra a inutilidade do dispositivo, assemelhando-se a um objeto inanimado. A prevenção do "*bricking*" reside na estrita observância das diretrizes do fabricante e na garantia de um processo de atualização ininterrupto e com o *firmware* correto.

7. **Verificação da Nova Versão:** Após a conclusão da atualização, o switch geralmente reinicia automaticamente ou solicita o reinício manual. Para garantir que o processo obteve sucesso é recomendado verificar a versão do *firmware* novamente na interface de gerenciamento.
8. **Testes:** Realizar testes básicos de conectividade e funcionalidades para garantir que o switch esteja operando corretamente com a nova versão do *firmware*.

Na Tabela 22 estão exemplos da configuração em switches diversos.

Tabela 22. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

switch>enable
switch#copy tftp: flash:
Address or name of remote host []? ***10.0.0.22***
Source filename []? ***c2960x-universalk9-mz.150-2.EX5.bin***
Destination filename [flash:/c2960x-universalk9-mz.150-2.EX5.bin]?

Faz o download do arquivo* ***c2960x-universalk9-mz.150-2.EX5.bin* *do servidor de TFTP com* ***IP 10.0.0.22*** *para a memória flash do switch*

switch#show boot
*switch#boot system flash:/****c2960x-universalk9-mz.150-2.EX5.bin***
switch# write memory
switch# reload

Lista as imagens de firmware, seleciona a nova imagem do firmware* ***c2960x-universalk9-mz.150-2.EX5.bin* *para ser usada no próximo reboot, salva a configuração e faz um reboot*

Huawei S5720-52X-LI (CLi)

<switch> tftp ***10.0.0.22*** *get* ***s5720li-v200r019c10spc500.cc***
<switch> tftp ***10.0.0.22*** *get* ***s5720li-v200r019sph010.pat***

Copia o arquivo de firmware* ***s5720li-v200r019c10spc500.cc* *do servidor de TFTP* ***10.0.0.22*** *e copia o arquivo de patch do firmware* ***s5720li-v200r019sph010.pat***

<switch> system-view
*[switch] startup system-software flash:/****s5720li-v200r019c10spc500.cc***
*[switch] startup patch flash:/****s5720li-v200r019sph010.pat***
[switch] commit
[switch] return

**Configura o novo firmware e o patch para serem utilizados na inicialização do próximo reboot*

<switch> reboot
<switch> display version

**Faz um reboot e o comando para verificar se o novo firmware foi instalado.*

Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Vty-1# copy tftp file
TFTP server IP address: ***10.0.0.22***
Choose file type:
1. config
2. opcode
Source file name: ***ECS2100_Jump_V117.8.8.1.bix***
Destination file name:
** Não é necessário trocar o nome do arquivo de destino*
Vty-1#configure
Vty-1(config)#boot system opcode: ***ECS2100_Jump_V117.8.8.1.bix***
Vty-1#exit
Vty-1#write
Vty-1#reload

** Este modelo, no firmware utilizado não possui as funcionalidades de atualização de firmware pela console web. Para realizar este procedimento é possível o acesso pela console em linha de comando por meio de Telnet.*

3com 2226 (Web)

3.13 Protocolos de Acesso Remoto

O acesso remoto ao switch poderá ser realizado por protocolos que incluem SSH (*Secure Shell*) para acesso seguro via linha de comando e/ou Telnet que realiza o mesmo acesso via linha de comando, mas menos seguro. A interface web (GUI) que faz uso do protocolo HTTP, disponível em quase a totalidade dos switches gerenciáveis, pode ser configurada para uso do HTTPS para melhorias na segurança. Na Tabela 23 estão exemplos da configuração em switches diversos.

Tabela 23. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Telnet
switch# configure terminal
switch(config)# line vty 0 15
switch(config-line)# transport input telnet
switch(config-line)# password senh@123
switch(config-line)# login
switch(config-line)# exit

SSH
switch# configure terminal
switch(config)# hostname switch123
switch123(config)# ip domain-name switch123.com
switch123(config)# crypto key generate rsa
// Durante a geração da chave, será perguntado o tamanho do módulo (ex: 1024, 2048)
// Escolha 1024 ou 2048 bits para melhor segurança.
switch123(config)# ip ssh version 2
// É altamente recomendável usar a versão 2 do SSH para maior segurança.
switch123(config)# line vty 0 15
switch123(config-line)# transport input ssh
// Ou 'transport input ssh telnet' se quiser Telnet também (não recomendado)
switch123(config-line)# login local
// Para usar contas de usuário locais criadas no switch.
switch(config-line)# exit
switch(config)# username aluno privilege 15 password !senhaAluno
// Cria um usuário local com privilégio 15 (acesso total).

HTTP e HTTPS
switch# configure terminal
switch(config)# ip http server
switch(config)# ip http secure-server
// Ativa o servidor HTTPS
switch(config)# crypto key generate rsa
// Será perguntado o tamanho do módulo, escolher 1024 ou 2048.
switch(config)# ip http authentication local
switch(config)# username aluno privilege 15 password !senhaAluno

Huawei S5720-52X-LI (CLi)

Telnet
<switch> system-view
[switch] telnet server enable
[switch] user-interface vty 0 4
[switch-ui-vty0-4] protocol inbound telnet
// Define o modo de autenticação para AAA (que pode ser local, RADIUS, etc.).
// Será usado o modo de autenticação local neste exemplo.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

[switch-ui-vty0-4] authentication-mode aaa
// Define o nível de privilégio para usuários que acessam via Telnet.
// 3 é o nível mais alto para usuários normais, semelhante ao 'privilege 15' da Cisco.
// Em alguns VRPs da switch, o nível de privilégio 15 é o máximo.
[switch-ui-vty0-4] user privilege level 3
[switch-ui-vty0-4] quit
// Entra no modo de configuração AAA para criar usuários locais.
[switch] aaa
// Cria um usuário local com senha criptografada irreversivelmente.
// 'irreversible-cipher' é mais seguro que 'cipher' (criptografia reversível).
[switch-aaa] local-user aluno password irreversible-cipher !senhaAluno
// Associa o usuário ao serviço Telnet.
[switch-aaa] local-user aluno service-type telnet
// Define o nível de privilégio do usuário local.
[switch-aaa] local-user aluno privilege level 3
[switch-aaa] quit
[switch] save

SSH
<switch> system-view
// Habilita o servidor STelnet (SSH) no switch.
[switch] stelnet server enable
// Habilita o servidor SFTP (transferência de arquivos pelo SSH) no switch.
[switch] sftp server enable
// Gera as chaves RSA locais para criptografia SSH.
// O switch perguntará o tamanho do módulo. 2048 é um bom valor para segurança.
[switch] rsa local-key-pair create
// Entra no modo de configuração das linhas VTY.
[switch] user-interface vty 0 4
// Permite o acesso SSH nas linhas VTY.
[switch-ui-vty0-4] protocol inbound ssh
// Define o modo de autenticação para AAA.
[switch-ui-vty0-4] authentication-mode aaa

// Define o nível de privilégio para usuários que acessam via SSH.
[switch-ui-vty0-4] user privilege level 3
[switch-ui-vty0-4] quit
// Entra no modo de configuração AAA.
[switch] aaa
// Cria um usuário local com senha criptografada.
[switch-aaa] local-user aluno password irreversible-cipher !senhaAluno
// Associa o usuário ao serviço SSH.
[switch-aaa] local-user aluno service-type ssh
// Define o nível de privilégio do usuário local.
[switch-aaa] local-user aluno privilege level 3

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

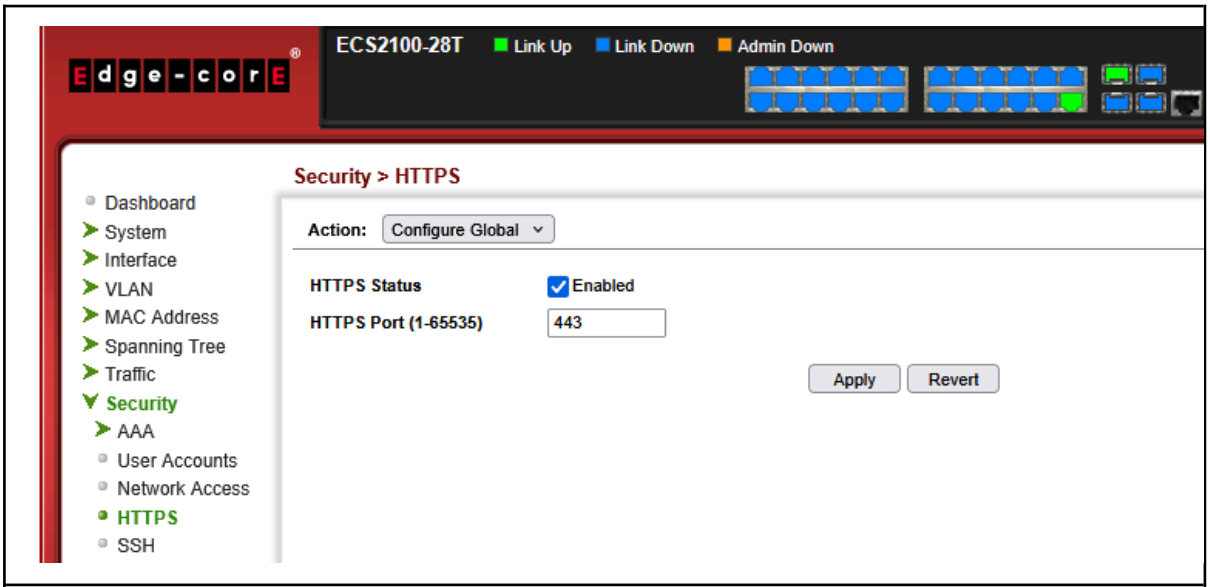
[switch-aaa] quit
// Define o tipo de autenticação do usuário SSH como senha.
[switch] ssh user aluno authentication-type password
// Especifica o tipo de serviço que o usuário SSH pode usar (STelnet).
[switch] ssh user aluno service-type stelnet
[switch] save

HTTP
<switch> system-view
// Habilita o servidor HTTP.
[switch] http server enable
[switch] aaa
[switch-aaa] local-user aluno password irreversible-cipher !senhaAluno
[switch-aaa] local-user aluno service-type http
[switch-aaa] local-user aluno privilege level 3
[switch-aaa] quit
[switch] save

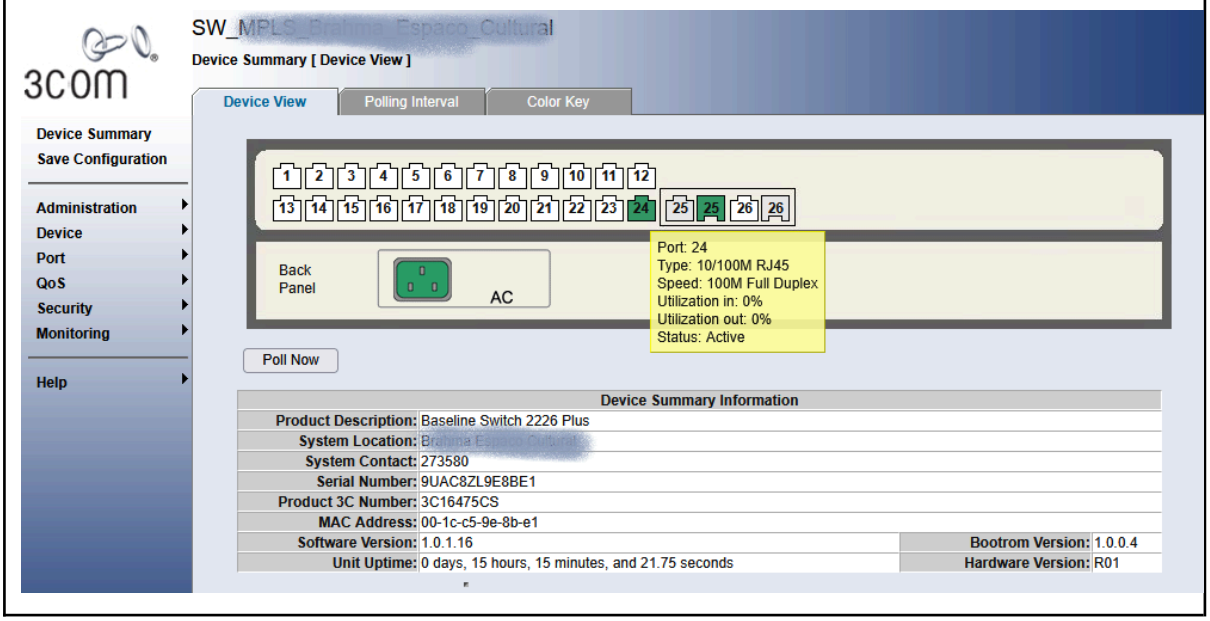
HTTPS
<switch> system-view
// Habilita o servidor HTTPS. (O servidor HTTP também precisa estar habilitado ou será habilitado automaticamente)
[switch] http secure-server enable
// Se ainda não foram geradas chaves RSA (para SSH), deverá ser gerada para uso do SSL/TLS no HTTPS. O switch perguntará o tamanho do módulo.
[switch] rsa local-key-pair create
[switch] aaa
[switch-aaa] local-user aluno password irreversible-cipher !senhaAluno
// 'http' aqui se refere ao serviço web em geral, tanto HTTP quanto HTTPS
[switch-aaa] local-user aluno service-type http
[switch-aaa] local-user aluno privilege level 3
[switch-aaa] quit
[switch] save

Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



3com 2226 (Web)



3.14 Usuários

O gerenciamento de contas de acesso ao switch permite definir diferentes níveis de privilégios para diferentes tipos de usuários, controlando quais configurações podem ser visualizadas e modificadas. A autenticação (nome de usuário e senha) garante que apenas pessoas autorizadas possam acessar e alterar as configurações do dispositivo.

A implementação de diferentes níveis de privilégios segue o princípio do menor privilégio, onde cada usuário recebe apenas os direitos de acesso necessários para realizar

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

suas tarefas específicas. Isso minimiza o risco de alterações acidentais ou maliciosas na configuração do switch. Alguns níveis de privilégios comuns incluem:

- **Modo de Usuário (*User Mode*):** Oferece acesso limitado a comandos básicos de visualização e testes simples. Usuários neste nível geralmente não podem alterar a configuração do switch.
- **Modo Privilegiado (*Privileged Mode ou Enable Mode*):** Fornece acesso completo a todos os comandos de configuração e gerenciamento do switch. Este nível geralmente é protegido por uma senha de "*enable*" que habilita configurações avançadas.
- **Níveis de Privilégio Personalizados:** Muitos switches gerenciáveis permitem a criação de níveis de privilégio personalizados, possibilitando a definição de um conjunto específico de comandos que um determinado grupo de usuários pode executar.

Na Tabela 24 estão exemplos da configuração em switches diversos.

Tabela 24. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

switch>enable
switch#conf t
switch(config)# snmp-server community public ro
switch(config)# username admin privilege 15 secret $SEnh@Pa$$w0rd
switch(config)# username monitor privilege 1 secret SEnh@Pa$$w0rd

** O nível 15 é para todos os privilégios e o nível 1 permite alguns comandos básicos.*

Huawei S5720-52X-LI (CLi)

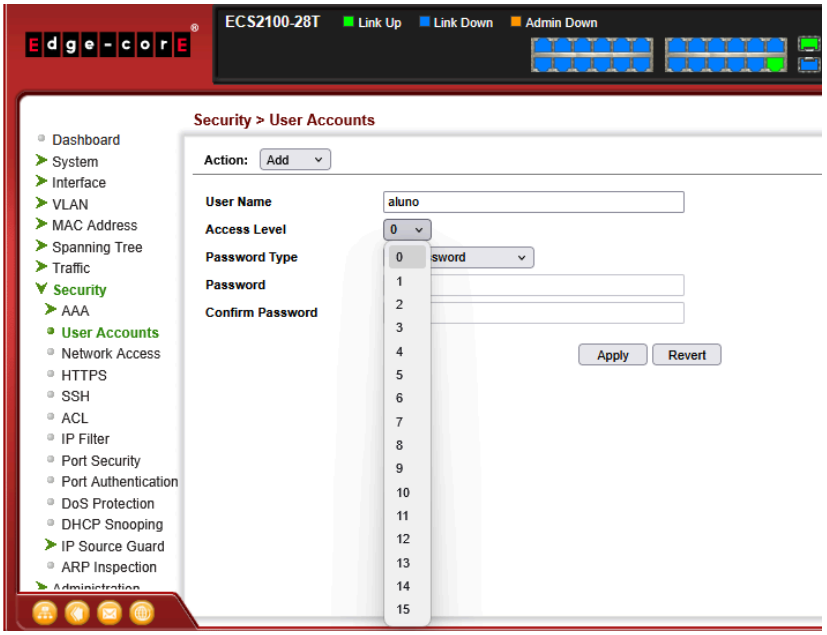
<switch> system-view
// Cria os usuários
[switch] aaa
[switch-aaa] local-user admin password irreversible-cipher $SEnh@Pa$$w0rd
[switch-aaa] local-user monitor password irreversible-cipher SEnh@Pa$$w0rd
// Define os privilégios e quais serviços serão permitidos ao usuário
[switch-aaa] local-user admin privilege level 15
[switch-aaa] local-user admin service-type ssh telnet terminal web
// Define os privilégios e quais serviços serão permitidos ao usuário
[switch-aaa] local-user monitor privilege level 1
[switch-aaa] local-user monitor service-type ssh

** Os níveis de privilégios são:*
0 (Visit level): Apenas comandos de diagnóstico (ping, tracert).
1 (Monitoring level): Comandos de monitoramento e manutenção do sistema (display).

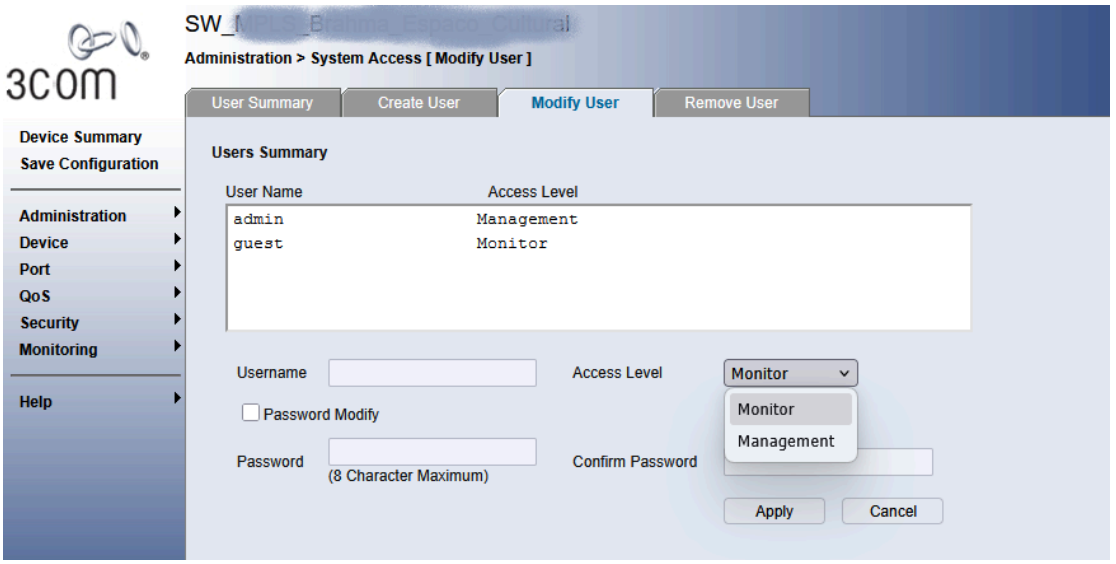
Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

2 (Configuration level): Comandos de configuração de serviço (ex: configuração de rotas). 3 (Management level): Comandos de operação básica do sistema, gerenciamento de usuários, depuração. É o nível mais alto para administradores completos (equivalente ao privilege 15 do Cisco para acesso total por padrão).

Edgecore ECS2100-28T (Web)



3com 2226 (Web)



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

3.15 Ferramentas de Diagnóstico

Estão disponíveis ferramentas de diagnóstico nos *firmwares* dos switches que auxiliam na identificação e solução de problemas de rede. São ferramentas comuns *ping* e *traceroute* em interfaces web e em linha de comando, Em linha de comando podem estar disponíveis também clientes dos protocolos Telnet e de SSH que possibilitam o acesso remoto de um switch para outro.

Ferramentas Básicas de Rede: Ping, Traceroute e ARP - https://youtu.be/Fiz2iUJ7YAA

Em alguns switches podem haver funcionalidades para testar a integridade dos cabos de rede conectados às suas interfaces, auxiliando na identificação de problemas físicos na camada 1. Na Tabela 25 estão exemplos da configuração em switches diversos.

Tabela 25. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

switch>enable
switch#ping 10.0.0.22
switch#traceroute 8.8.8.8
// Teste de cabo
switch#test cable-diagnostics tdr interface gi1/0/5
switch#show cable-diagnostics tdr interface g1/0/5

** Exemplo de saída do comando de diagnósticos de cabos:*

TDR test last run on: June 08 10:14:56

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
Gi1/0/5	1000M	Pair A	60 +/- 10 meters	Pair B	Normal
		Pair B	60 +/- 10 meters	Pair A	Normal
		Pair C	60 +/- 10 meters	Pair D	Normal
		Pair D	60 +/- 10 meters	Pair C	Normal

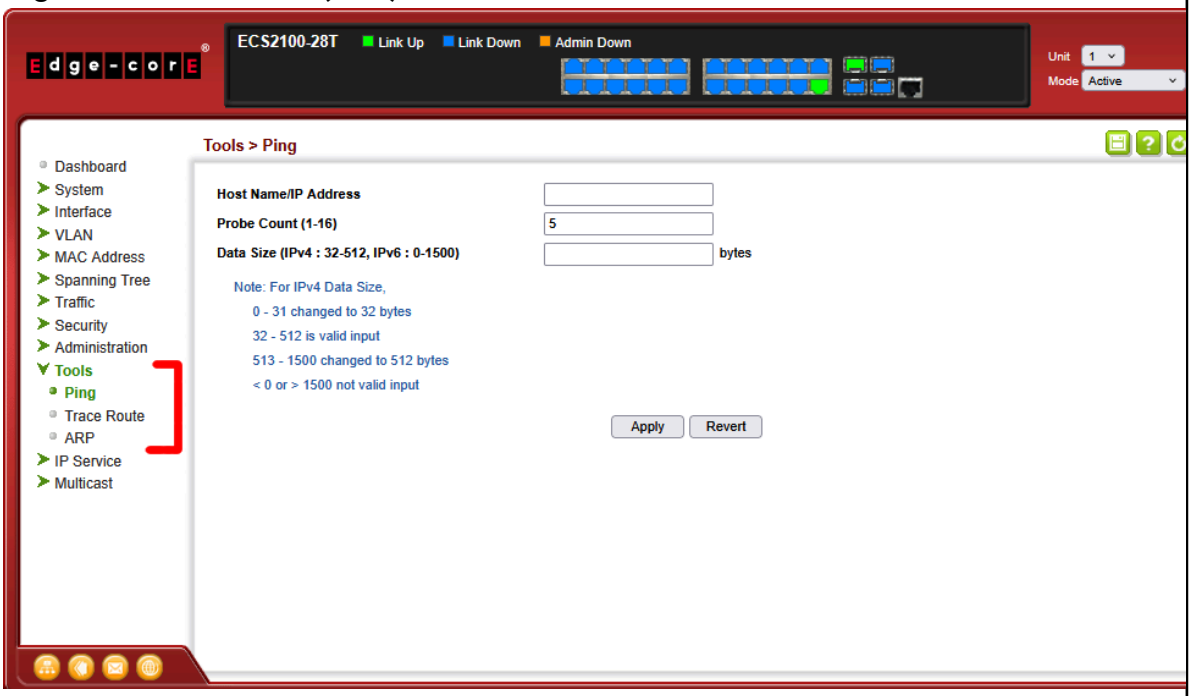
Huawei S5720-52X-LI (CLi)

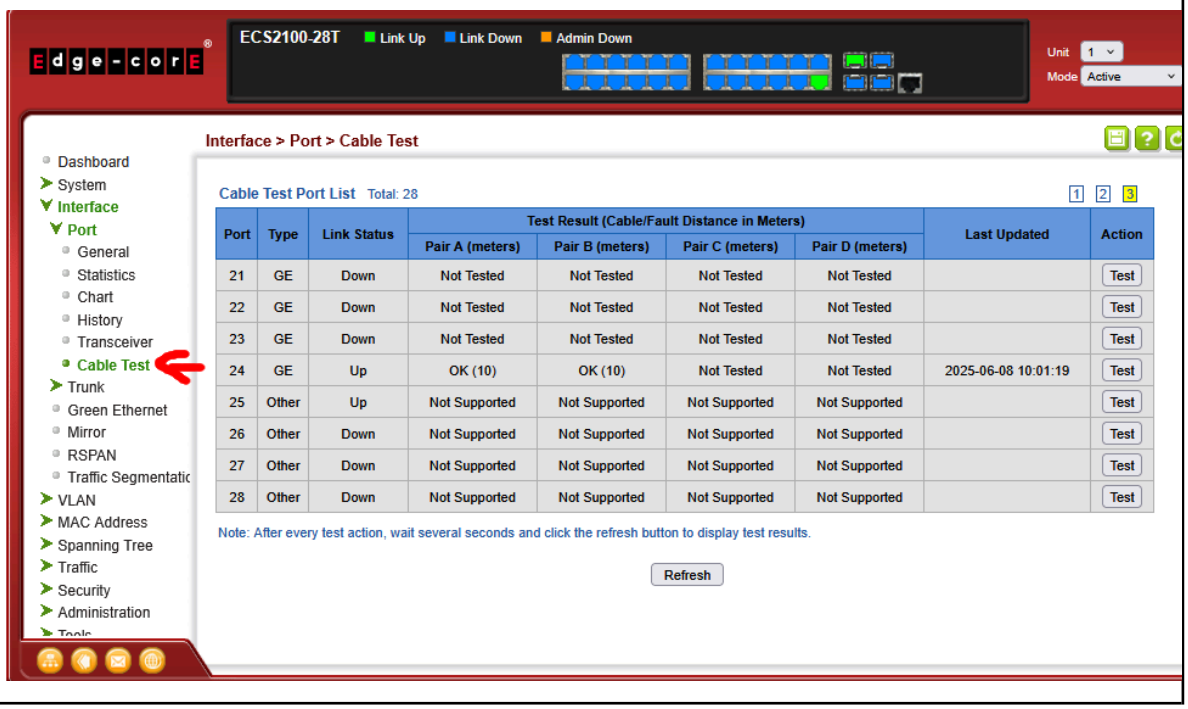
<switch>ping 10.0.0.22
<switch> traceroute 8.8.8.8

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

// Teste de cabo
<switch> system-view
[switch] interface GigabitEthernet0/0/5
[switch-GigabitEthernet0/0/5] virtual-cable-test

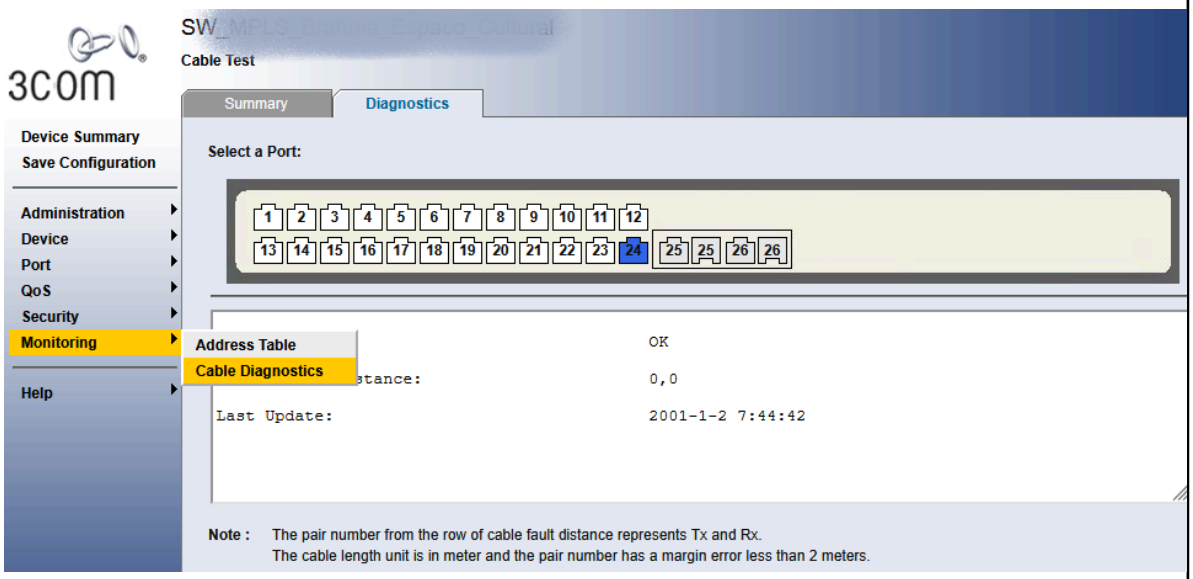
Edgecore ECS2100-28T (Web)





Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

3com 2226 (Web)



** Este modelo não possui as ferramentas ping e traceroute*

3.16 Reboot/Reset to Factory Defaults

A reinicialização, ou simplesmente *reboot ou reset*, consiste em desligar e ligar o switch, reiniciando o sistema operacional e todos os seus processos. Este procedimento é frequentemente utilizado para resolver problemas temporários de software, como lentidão no processamento, falhas em serviços específicos ou após a aplicação de certas configurações ou atualizações de *firmware* que exigem um reinício para serem ativadas completamente.

A reinicialização geralmente preserva a configuração atual do switch, armazenada na memória não volátil (como a NVRAM ou *flash memory*), se estiver sido salva previamente. Após o *reboot*, o switch carrega novamente a configuração salva e retorna ao seu estado operacional anterior (com as últimas configurações aplicadas). O procedimento de reboot poderá ser feito via software, por meio da interface de gerenciamento, fazendo um ciclo de desliga/liga energia ou por meio de algum botão disponível no switch. Um pressionamento curto e rápido neste botão geralmente inicia um *reboot* do dispositivo. É importante consultar o manual do fabricante para confirmar o comportamento específico do botão de reset. Na Figura 27 um exemplo de botão de reset em um switch HP modelo Aruba 1930.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Figura 27. Botão de reset em um switch HP modelo Aruba 1930.

O procedimento de restauração às configurações de fábrica (*Reset to Factory Defaults*), ou simplesmente *reset* de fábrica, é uma operação mais drástica que apaga todas as configurações personalizadas previamente aplicadas no switch, retornando-o ao seu estado original, tal como saiu da fábrica. Isso inclui configurações de VLANs, endereços IP, senhas, configurações de segurança e qualquer outra personalização realizada.

O *reset* de fábrica é útil em diversas situações:

- **Recuperação de Senhas Perdidas:** Se a senha de acesso ao switch for esquecida, um *reset* de fábrica geralmente restaura as credenciais padrão do fabricante, permitindo o acesso para reconfiguração.
- **Solução de Problemas Persistentes:** Em casos onde o switch apresenta um comportamento anômalo e a causa não pode ser identificada, um *reset* de fábrica pode eliminar configurações corrompidas ou conflitantes.
- **Reutilização ou Descarte do Switch:** Antes de reutilizar o switch em outra rede ou descartá-lo, é fundamental realizar um *reset* de fábrica para remover todas as configurações sensíveis.

A restauração às configurações de fábrica geralmente é realizada através de um procedimento específico envolvendo o botão de reset físico ou com um comando pela interface de gerenciamento. No caso do uso de um botão físico, o manual do fabricante deverá ser consultado para consultar sobre o tempo exato e o comportamento esperado das luzes indicadoras durante o processo de *reset*. Na Tabela 26 estão exemplos da configuração em switches diversos.

Tabela 26. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

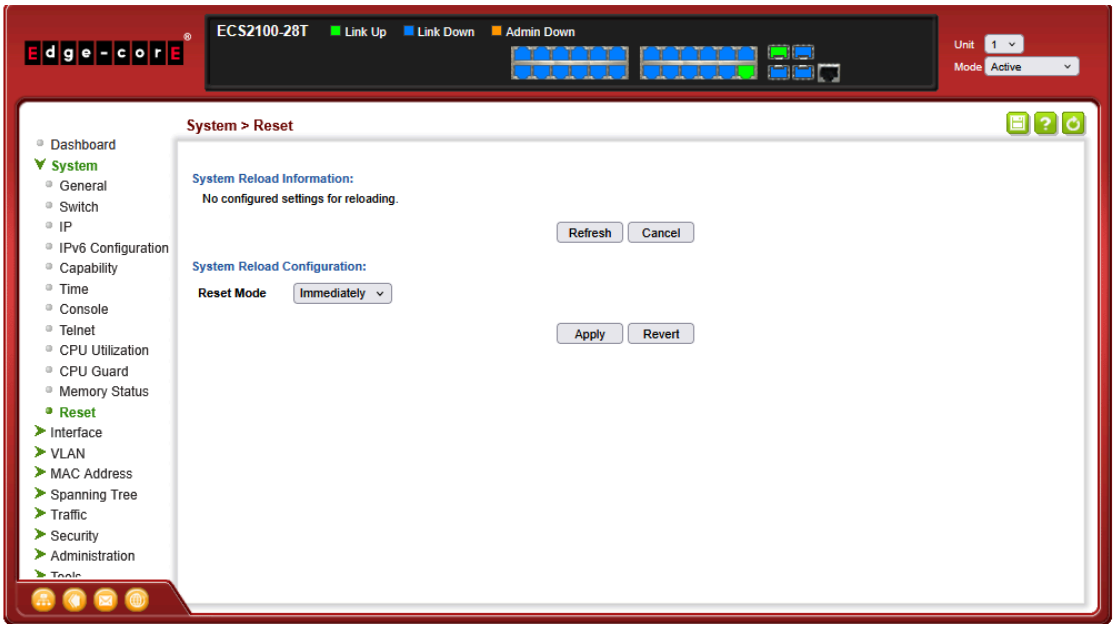
Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

switch>enable
switch#erase startup-config
switch#delete flash:vlan.dat
switch#reload
** Caso solicite a gravação da configuração atual antes de fazer o reboot, optar por não salvar*

Huawei S5720-52X-LI (CLi)

<switch> reset saved-configuration
<switch> reboot

Edgecore ECS2100-28T (Web)

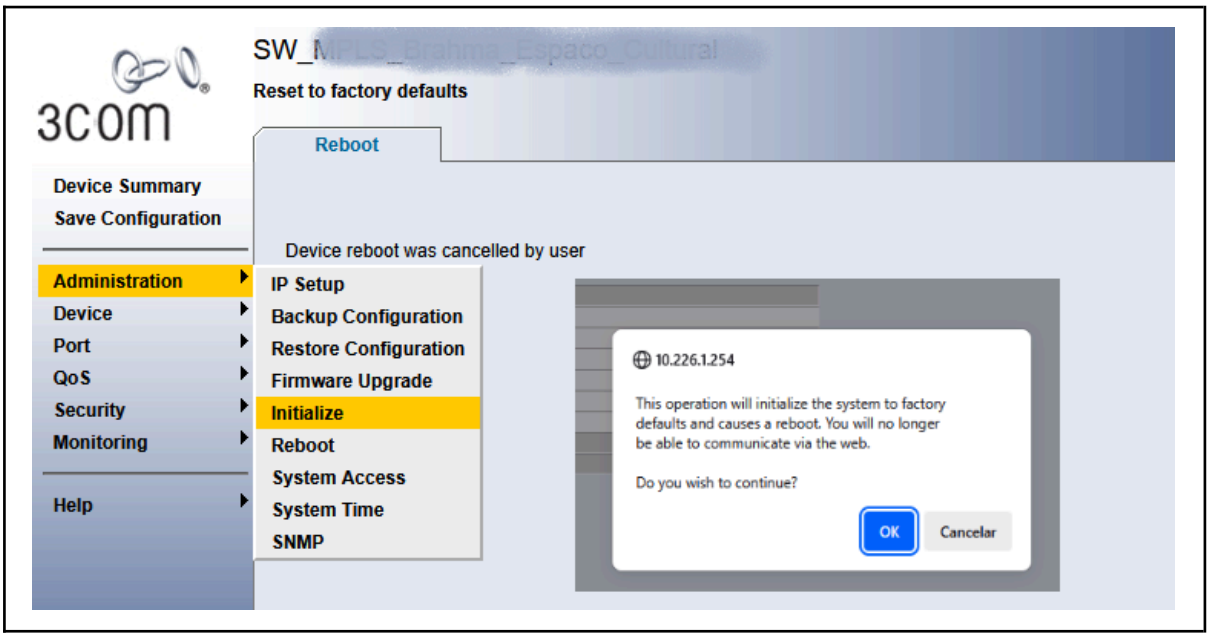


// Restauração para o padrão de fábrica
Vty-1#configure
Vty-1(config)#boot system config:Factory_Default_Config.cfg
Vty-1(config)#exit
Vty-1#reload

* Este modelo não possui a funcionalidade de restauração para o padrão de fábrica na interface web.

3com 2226 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

4) VLAN (Virtual LAN)

A VLAN (*Virtual LAN*) é um domínio de broadcast logicamente particionado e isolado na camada de enlace de dados do modelo OSI (camada 2). As VLANs permitem que sejam agrupados hosts mesmo que não estejam diretamente conectados ao mesmo switch. A evolução das VLANs tem sido fundamental para atender à crescente complexidade e às demandas de redes corporativas, data centers e ambientes de nuvem, otimizando recursos, aprimorando a segurança e simplificando o gerenciamento de rede.

As primeiras redes locais (LANs) eram frequentemente baseadas em hubs, dispositivos que operam na camada física e conectam todos os dispositivos em um único domínio de colisão e broadcast. Nessa arquitetura, qualquer mensagem enviada por um dispositivo era replicada para todas as outras portas do hub, resultando em problemas de desempenho e escalabilidade à medida que o número de dispositivos na rede aumentava. Com o uso de switches os problemas de desempenho relacionados ao compartilhamento do meio físico foram resolvidos, mas os domínios de broadcast não. A solução para criar vários domínios de broadcast, antes da VLANs, era com o uso de roteamento entre os segmentos da rede local.

O tráfego de broadcast, necessário para diversas funções de rede, como descoberta de serviços e resolução de endereços, crescia linearmente com o número de dispositivos, consumindo largura de banda e poder de processamento desnecessariamente. Além disso, a falta de segmentação lógica significava que todos os dispositivos compartilham o mesmo espaço de rede, independentemente de sua função ou afiliação departamental, levantando preocupações de segurança e dificultando a aplicação de políticas de acesso granular.

O desenvolvimento da tecnologia VLAN foi motivado pela necessidade de superar essas limitações inerentes às LANs tradicionais. A escalabilidade tornou-se uma preocupação central, pois as redes locais corporativas lutavam para manter um desempenho aceitável com um número crescente de dispositivos. As VLANs permitiram que uma única rede física fosse dividida logicamente em múltiplas redes virtuais, cada uma operando como seu próprio domínio de broadcast independente. Essa segmentação limitou o alcance do tráfego de broadcast, reduzindo a carga em dispositivos individuais e melhorando a eficiência geral da rede.

A segurança foi outra motivação fundamental para a criação das VLANs. Em uma LAN, todos os dispositivos estavam no mesmo segmento de rede, o que significava que um acesso não autorizado ou uma vulnerabilidade em um único dispositivo poderia potencialmente comprometer toda a rede. As VLANs introduziram a capacidade de criar limites de segurança lógicos, isolando diferentes grupos de usuários ou departamentos e restringindo a comunicação entre eles, a menos que explicitamente permitido.

O gerenciamento do tráfego de broadcast também se tornou um fator crítico. Em redes maiores, o volume de mensagens de broadcast poderia levar ao congestionamento e à degradação do desempenho. As VLANs ofereceram uma solução eficaz para conter a

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

propagação de broadcasts, garantindo que fossem entregues apenas aos dispositivos que realmente precisavam recebê-los, otimizando assim o uso da largura de banda disponível.

VLAN: Conceitos Básicos - https://youtu.be/xZ-SOGYkafA

4.1 Primeiro Padrão Formal (IEEE 802.1Q)

O primeiro padrão formal para a implementação VLANs em redes Ethernet foi o IEEE 802.1Q. Publicado pela primeira vez em 1998 pelo IEEE (*Institute of Electrical and Electronics Engineers*), este padrão definiu um sistema de *tagging* para *frames* (quadros) Ethernet, permitindo que a funcionalidade VLAN fosse implementada em infraestruturas de rede existentes, mantendo a compatibilidade com dispositivos que não eram compatíveis com VLANs. Antes do IEEE 802.1Q, existiam soluções proprietárias para VLANs, como o *Inter-Switch Link* (ISL) da Cisco. Os principais objetivos do padrão IEEE 802.1Q incluíam:

- **Segmentação de Rede:** Criar múltiplas redes logicamente separadas em uma única infraestrutura física.
- **VLANs *Cross-Device*:** Permitir que as VLANs se estendessem por múltiplos dispositivos de rede, como switches.
- **Compatibilidade retroativa:** Assegurar a compatibilidade com dispositivos de rede mais antigos que não suportavam VLANs.
- **Otimização de Desempenho:** Melhorar a eficiência da rede através da limitação dos domínios de broadcast.
- **Aprimoramento da Segurança:** Aumentar a segurança da rede através do isolamento lógico do tráfego entre diferentes VLANs.

O padrão IEEE 802.1Q alcança a funcionalidade VLAN através da adição de um *tag* de 4 bytes ao *frame* Ethernet padrão. Este *tag* é inserido entre o endereço MAC de origem e o campo EtherType do *frame* original. O *tag* 802.1Q contém campos de controle que estão listados na Tabela 27.

Tabela 27. Campos de controle do padrão IEEE 802.1Q

Campo	Tamanho (bits)	Descrição
Tag Protocol Identifier (TPID)	16	Valor 0x8100 que identifica o *frame* como marcado (*tagged*) 802.1Q
Priority Code Point (PCP)	3	Especifica a prioridade do *frame* para Qualidade de Serviço (QoS)
Drop Eligible Indicator (DEI)	1	Indica se o *frame* é elegível para descarte em caso de congestionamento

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

VLAN Identifier (VID)	12	Identifica exclusivamente a VLAN à qual o *frame* pertence, permitindo até 4094 VLANs (total de 4096, sendo a VLAN ID 0 e a 4095 não utilizáveis)

A adição deste *tag* aumenta o tamanho máximo do *frame* Ethernet padrão de 1518 bytes para 1522 bytes, alterando o MTU (*Maximum Transfer Unit*). O campo TPID (*Tag Protocol Identifier*) com o valor 0x8100 sinaliza para os dispositivos de rede compatíveis com 802.1Q que o *frame* contém informações de VLAN nos próximos bytes. O campo TCI (*Tag Control Information*) é subdividido em PCP (*Priority Code Point*), que permite a priorização do tráfego, DEI (*Drop Eligible Indicator*), que auxilia no gerenciamento de congestionamento, e VID (*VLAN Identifier*), que efetivamente segmenta a rede em até 4094 VLANs lógicas (as VLANs 0 e 4095 são reservadas e não usadas), em um espaço de endereçamentos de 2^12 de vai do 0 até o 4095, sendo o total de 4096 identificadores de VLANs.

4.2 Avanços e Adições aos Padrões de VLAN

Após a publicação do padrão IEEE 802.1Q, o conceito de VLAN evoluiu com a introdução de diferentes métodos de associação e tipos de VLANs para atender a necessidades específicas de rede.

As **VLANs Baseadas em Porta** foram uma das primeiras implementações, onde a associação de um dispositivo a uma VLAN é determinada pela porta do switch à qual ele está fisicamente conectado. Todos os dispositivos conectados a uma porta configurada para uma VLAN específica são automaticamente membros dessa VLAN. Este método é simples de configurar e é adequado para ambientes onde os usuários e recursos permanecem conectados às mesmas portas do switch, sendo comumente usado para separar departamentos ou tipos de dispositivos, como uma VLAN para o departamento de marketing e outra para o departamento financeiro. É a forma mais comum de aplicação de VLANs em redes locais corporativas.

As **VLANs Baseadas em MAC** oferecem maior flexibilidade, pois a associação de um dispositivo a uma VLAN é baseada no seu endereço MAC. O switch mantém uma tabela que mapeia endereços MAC para VLANs. Quando um dispositivo se conecta à rede, o switch examina seu endereço MAC e o associa à VLAN configurada para esse endereço, independentemente da porta do switch utilizada. Isso facilita a movimentação de dispositivos dentro da rede sem a necessidade de reconfigurar as VLANs no switch.

As **VLANs Dinâmicas** proporcionam um nível ainda maior de automação. A associação de um dispositivo a uma VLAN é determinada dinamicamente com base em critérios como o endereço MAC do dispositivo ou as credenciais do usuário. Um servidor centralizado, como um VMPS (*VLAN Membership Policy Server*) da Cisco, pode ser usado para gerenciar essas associações dinâmicas. Quando um novo dispositivo se conecta à rede,

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

o switch consulta o VMPS para determinar a VLAN apropriada para esse dispositivo com base em seu endereço MAC. Outros métodos de atribuição dinâmica incluem a autenticação baseada no padrão IEEE 802.1X, onde a VLAN de um usuário é atribuída com base em suas credenciais de login. Por exemplo, quando um funcionário conectar seu notebook corporativo à rede, o switch o autentica via 802.1X. O servidor RADIUS verifica as credenciais do usuário (obtidas do Microsoft Active Directory, por exemplo) e o endereço MAC do notebook. Com base nessas informações, o servidor RADIUS instrui o switch a atribuir o notebook à vlan alocada para uso de funcionários.

As **VLANs de Voz (*Voice* VLANs)** foram desenvolvidas para otimizar o desempenho do tráfego de voz sobre IP (VoIP). Uma VLAN separada é criada especificamente para o tráfego de voz, permitindo que ele receba tratamento prioritário através de mecanismos de Qualidade de Serviço (QoS). Os switches configurados com VLANs de voz podem identificar pacotes de voz (geralmente através de seus endereços MAC de origem ou protocolos) e atribuir-lhes maior largura de banda e menor latência. O campo PCP (*Priority Code Point)* no *tag* 802.1Q é frequentemente usado para marcar pacotes de voz com uma prioridade mais alta, garantindo a qualidade das chamadas de voz. Na Tabela 28 há um resumo dos tipos de VLANs, critérios de associação e cenários de uso típicos.

Tabela 28. Resumo dos tipos de VLANs

Tipo de VLAN	Critério de Associação	Cenários de Uso Típicos
Baseada em Porta	Porta do Switch	Departamentos, dispositivos estáticos, redes pequenas e médias.
Baseada em MAC	Endereço MAC	Mobilidade de dispositivos, redes com usuários que se conectam a diferentes pontos.
Dinâmica	Endereço MAC/Credenciais	Grandes redes, ambientes com movimentação frequente de dispositivos e usuários, segurança aprimorada.
Voice VLAN	Tipo de Tráfego	Priorização de tráfego VoIP, garantia de qualidade de chamadas em redes com telefonia IP.

4.3 Interconexão de VLANs

Para que as VLANs se tornassem uma solução escalável para redes maiores, era essencial um mecanismo para permitir a comunicação entre VLANs que se estendiam por múltiplos switches. O *trunking* resolve essa necessidade, permitindo que um único link físico entre switches transporte o tráfego de múltiplas VLANs simultaneamente. Sem o *trunking*, seria necessário um link físico separado para cada VLAN que precisasse abranger vários switches, o que seria ineficiente, aumentaria a complexidade e os custos de cabeamento.

O padrão IEEE 802.1Q desempenhou um papel fundamental no *trunking* de VLANs. As

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

portas de switch configuradas como *trunk ports* (portas tronco) são capazes de enviar e receber tráfego *tagged* com identificadores de VLAN (VIDs) diferentes. Quando um *frame* precisa ser encaminhado de um switch para outro através de uma porta tronco, o *tag* 802.1Q contendo o VID é preservado. O switch receptor lê esse *tag* e encaminha o *frame* para a VLAN apropriada. Isso padronizou o processo de *trunking*, garantindo a interoperabilidade entre equipamentos de diferentes fabricantes e permitindo a construção de redes VLAN complexas e escaláveis.

Antes da ampla adoção do IEEE 802.1Q, a Cisco desenvolveu sua própria tecnologia proprietária de *trunking,* o ISL (*Inter-Switch Link*). O ISL é um protocolo que encapsula o *frame* Ethernet original com um cabeçalho e um *trailer*, adicionando informações de VLAN. Embora eficaz em ambientes compostos exclusivamente por equipamentos Cisco, o ISL não é um padrão aberto e não é suportado por switches de outros fabricantes. Com a crescente aceitação do IEEE 802.1Q como padrão para *trunking*, o uso de tecnologias proprietárias como o ISL foi descartado, pois o 802.1Q oferece uma solução interoperável e mais flexível para ambientes de rede heterogêneos. Na Tabela 29 está um comparativo entre as soluções para VLANs aberta e proprietária.

Tabela 29. Comparativo entre IEEE 802.1Q e Cisco ISL

Característica	**IEEE 802.1Q**	**Cisco ISL**
Padrão	Aberto (IEEE)	Proprietário (Cisco)
Fabricante Principal	*Multi-vendor*	Cisco
Método de *Tagging*	Inserção de *tag* de 4 bytes no frame Ethernet	Encapsulamento do *frame* Ethernet com cabeçalho e *trailer*
Suporte a Outros Fabricantes	Sim	Não

Quando um quadro ethernet precisa trafegar por uma porta *trunk*, ele é modificado para incluir uma *tag* de VLAN. Essa tag é inserida no quadro original, o que aumenta o tamanho do quadro e altera seus dados. Consequentemente, o valor do *Frame Check Sequence* (FCS), que contém o *Cyclic Redundancy Check* (CRC), deve ser recalculado. O CRC é um valor de 32 bits calculado pelo dispositivo de origem com base em todos os bytes do quadro, excluindo o próprio campo FCS. Ele serve para verificar a integridade dos dados durante a transmissão. Qualquer alteração em um único bit do quadro resultará em um CRC diferente, indicando uma possível corrupção dos dados.

No momento que um switch recebe um quadro Ethernet que precisa ser enviado por uma porta *trunk* configurada com VLANs, o switch insere um cabeçalho no padrão IEEE 802.1Q. Este cabeçalho é composto por um campo TPID (*Tag Protocol Identifier*) de 2 bytes e um campo TCI (*Tag Control Information*) de 2 bytes, totalizando 4 bytes. Essa inserção ocorre logo após o campo Endereço de Origem (*Source Address*) e antes do campo Tipo (*EtherType*) original. A adição da *tag* de VLAN altera o conteúdo total do quadro. Com os 4 bytes adicionais e a modificação da estrutura do quadro, o padrão de bits que o switch usa para calcular o CRC original é invalidado.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Devido a essa alteração de conteúdo, o switch transmissor (aquele que insere a *tag* de VLAN) deve recalcular o CRC para todo o quadro modificado, incluindo a *tag* de VLAN recém-adicionada. O novo valor de CRC é então inserido no campo FCS antes que o quadro seja transmitido pela porta *trunk*. Este processo consome recursos de processamento do switch e poderá limitar a taxa de comutação em modelos de switches com poucos recursos computacionais.

Quando um switch receptor (ou outro dispositivo de rede) recebe um quadro com *tag* de VLAN, ele também realiza o cálculo do CRC sobre todo o quadro (incluindo a *tag*) e compara o resultado com o valor presente no campo FCS. Se os valores coincidirem, o quadro é considerado íntegro. Em seguida, dependendo da configuração da porta, o switch pode remover a *tag* de VLAN (se for uma porta de acesso para uma VLAN específica) antes de encaminhar o quadro internamente ou para o dispositivo final, ou ele pode encaminhá-lo com a *tag* (para outra porta *trunk*, por exemplo).

O recálculo do FCS é fundamental para manter a integridade dos dados em redes que utilizam VLANs. Sem ele, a adição da tag 802.1Q faria com que o CRC original fosse inválido, levando a quadros descartados no destino e a falhas na comunicação. Garante-se, assim, que a funcionalidade de verificação de erros continue operante, mesmo com as modificações estruturais introduzidas pelas *tags* de VLAN. É importante ressaltar que o processo de recálculo do CRC é transparente para o usuário final, sendo uma operação interna do switch que lida com o tráfego de VLANs.

4.4 Conceitos Relacionados que Ampliaram as Capacidades das VLANs

As capacidades das VLANs foram ainda mais ampliadas com a introdução de conceitos relacionados, como VLANs privadas e VLANs de gerenciamento.

As **VLANs Privadas** permitem um isolamento mais granular de hosts dentro do mesmo espaço de endereçamento da camada 2. Uma VLAN privada é dividida em uma VLAN primária e uma ou mais VLANs secundárias. As portas em uma VLAN privada podem ser configuradas como promíscuas *(promiscuous)*, *isoladas* (*isolated)* ou *comunitárias* (*community)*. Portas promíscuas podem se comunicar com todas as outras portas na VLAN privada, incluindo as isoladas e comunitárias. Portas *isoladas* só podem se comunicar com portas promíscuas, enquanto portas comunitárias podem se comunicar entre si e com portas promíscuas, mas não com portas *isoladas*. Este conceito é particularmente útil em ambientes como hospedagem compartilhada ou redes de acesso público, onde é necessário isolar logicamente dispositivos dentro da mesma sub-rede para segurança e controle.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

As **VLANs de Gerenciamento** são VLANs separadas criadas especificamente para o tráfego de gerenciamento de rede. Ao segregar o tráfego de protocolos como SNMP, SSH e Telnet em uma VLAN dedicada, os administradores de rede podem proteger o acesso aos dispositivos de gerenciamento da rede, separando-o do tráfego de dados normal do usuário. Isso melhora a segurança, pois o acesso administrativo pode ser controlado e restrito a um conjunto específico de hosts autorizados, reduzindo o risco de acesso não autorizado e aumentando a resiliência da infraestrutura de rede. A VLAN 1 é a padrão nos dispositivos e, geralmente, é usada como VLAN para gerenciamento.

4.5 Aplicação Prática de VLANs em Redes Corporativas

A aplicação de VLANs em redes corporativas é um procedimento essencial para a administração do ambiente. Os critérios para a criação de VLANs são baseados nos tipos de usuários, por exemplo visitantes, clientes ou colaboradores, que deverão ficar isolados uns dos outros. Outro critério é a questão da localização, por exemplo prédios ou andares distintos. Um outro critério bastante comum é a definição de VLAN por tipo de aplicação ou serviço, por exemplo câmeras de vídeo, rede sem fios, impressoras, gerenciamento de dispositivos, servidores de arquivos entre outros.

VLANs: resolução de avaliação - https://youtu.be/UmYe65w7Cd8

A implementação das VLANs começa com a definição das identificações de cada VLAN, criação do VID, que é numérico e vai do 1 ao 4094, sendo a 0 e 4095 reservadas (em alguns switches a restrições de quais VID podem ser usados e de quantas VLAN simultâneas podem ser criadas). Os quadros marcados possuem mais 4 Bytes, com isto o tamanho máximo dos quadros passa a ser de 1522 Bytes. Portanto, os dispositivos que recebem pacotes com 4 Bytes, devem ter compatibilidade com VLANs. Em caso contrário, a interface de rede identifica o pacote com um *giant* (gigante) por exceder o MTU (*Maximum Transfer Unit*) padrão da rede Ethernet que é de 1518 Bytes. Com o uso de *jumbo frames,* de cerca de 9 KB de tamanho, o cabeçalho maior usado nos pacotes de VLAN torna-se irrelevante em relação ao *overhead*.

A relação VID e endereços IPv4 e IPv6 é uma boa prática na administração de redes. Por exemplo, ao definir uma VLAN para o prédio 30, o VID poderia ser 30 e o endereçamento IPv4 10.30.0.0/16 e o endereçamento IPv6 algo como 2001:DB8:AAAA:30::/64. Desta forma, ao receber um IP dentro destas faixas será possível identificar de qual VLAN pertence. Nos switches utilizam-se nomes para identificar as VLANs. Estes nomes têm apenas função de uma descrição da VLAN, o que importa é a identificação do VID. Portanto, no caso de ser

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

criada a VLAN “Predio30” com a VID 30 em um switch e em outro criar a VLAN 30 com o nome “Abacaxi”, não haverá nenhum problema no protocolo. Entretanto, manter o mesmo padrão de nomes de VLANs entre os switches é algo importante e deve ser feito para melhorar a administração do ambiente.

Projeto Lógico de Redes: Dicas sobre Endereçamento/VLANs - https://youtu.be/Fxg9FAikKe8

As VLANs só terão efeito se forem aplicadas nas portas dos switches. Por padrão, todas as portas do switch estão na VLAN 1 e o tipo de porta acesso (*untagged*). Assim, todas as portas têm comunicação direta e participam da mesma rede. Ao aplicar uma VLAN diferente em uma porta, por exemplo VLAN 30, o equipamento conectado a esta porta passará para o domínio de broadcast da VLAN 30, não sendo mais acessível diretamente pelas demais portas que estão na VLAN 1. Basicamente, as portas com VLANs podem ser:

- ***Tagged*** (Modo Tronco) – quando o *host* ligado a porta do switch marca os pacotes (Ex.: roteadores, switches, APs)
- ***Untagged*** (Modo Acesso)– quando o host ligado a porta ignora a marcação de VLAN (Ex.: computadores de usuários)

As portas de *uplink*, que interligam switches, necessitam estar em modo tronco para possibilitar a passagem de múltiplas VLANs entre os switches. As VLANs podem ser permitidas ou bloqueadas entre os switches de forma administrativa. O caso mais comum é que seja realizada a configuração de quais VLANs necessitam ser informadas nas portas envolvidas no *uplink*, com a necessidade das VLANs serem iguais entre os switches interconectados. As portas em modo acesso são utilizadas para conexão de dispositivos que recebem os quadros não marcados (*untagged*) e não diferenciam VLANs. Algumas interfaces de rede podem não possuir suporte a VLANs e ignoram a marcação. Isto é muito raro atualmente, mas interfaces de rede antigas podem não ser compatíveis

Em caso de dispositivos que possuem conexões de múltiplas VLANs, por exemplo roteadores, *access points*, switches, as portas são em modo tronco (*tagged*) porque o dispositivo saberá separar o tráfego de cada VLAN. Em alguns equipamentos as portas do tipo *trunk* são usadas para montar agregação de portas. Portanto, é importante consultar a documentação do modelo do switch para verificar como realizar as configurações de VLANs. Na Tabela 30, um resumo dos tipos de portas que utilizam VLANs e quais tipos de dispositivos são conectados nestas portas.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Tabela 30. Resumo dos Tipos de Portas

Modo	Funcionalidade	Dispositivos Conectados
Acesso (*Access*)	A porta é membro de somente uma VLAN (considera a VLAN nativa da porta) Portas de acesso são usadas para conectar dispositivos finais e geralmente têm um PVID configurado para uma VLAN específica	Computadores, Impressoras, Câmeras IP
Tronco (*Trunk*)	A porta é capaz de suportar múltiplas VLANs Portas tronco são usadas para conectar outros switches ou dispositivos de rede e podem transportar várias VLANs	Switches, APs, roteadores, controladoras de APs, Servidores, Storages
Híbrido (*Hybrid*)	Uma porta em modo híbrido pode ser usada para conectar ao mesmo tempo equipamentos finais que não identificam *tags* e equipamentos que identificam *tags*	Telefone IP: a VLAN de telefonia marcada e um PC ligado ao telefone que não entende marcações Access Point: VLAN de gerenciamento do AP marcada e VLAN de uso para dados de usuários wireless untagged

O PVID (*Private VID*) é um identificador numérico associado a uma porta de switch que define a VLAN padrão para essa porta. Isso significa que todo o tráfego que chega a essa porta sem marcação (sem informações de VLAN específica) será associado à VLAN com o número de ID especificado como PVID. Uma porta de acesso terá o PVID único da VLAN a qual pertence o dispositivo conectado.

Todo o switch que possui suporte a VLAN, vem com todas as portas definidas na VLAN *default* (padrão). Normalmente, a VLAN *default* tem o VID igual a 1 e não pode ser

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

removida do switch. Em alguns casos de switches, é possível trocar a VLAN 1 para outra VLAN. Esta VLAN é usada para ser a VLAN de gerenciamento. Em caso de um switch perder a configuração, na configuração de fábrica todas as portas estão na VLAN 1.

O objetivo principal da *Voice VLAN* é separar o tráfego de voz (geralmente VoIP) do tráfego de dados em uma rede. Isso é feito para garantir que o tráfego de voz seja tratado com prioridade e qualidade adequada. A forma de associação é baseada no endereço MAC do telefone VoIP descoberto na porta ou pelo protocolo LLDP. Em caso de telefones IP com portas para compartilhamento de ponto de rede com computadores usa-se portas do tipo híbrida no switch e são passadas as VLANs de voz e de dados.

O QinQ, definido no padrão IEEE 802.1ad, se refere a uma técnica de encapsulamento de VLANs que tem a capacidade de empilhar VLANs em cima de outras VLANs. O nome é devido ao uso de duas *tags* do padrão IEEE 802.1q que define VLANs. Essa técnica é comumente usada em provedores de Internet e data centers. Para segmentar o tráfego de clientes em VLANs adicionais, fornecendo assim maior isolamento e flexibilidade. Com o QinQ há o aumento da quantidade de VLANs possíveis 2^12 x 2^12 = ~ 16 Milhões de VLANs. Um exemplo de aplicação seria a passagem da VLAN 1 de vários clientes na infraestrutura de um provedor ou qualquer outra VLAN repetida em um cliente que deva ser repassada em uma infraestrutura compartilhada.

Para haver comunicação entre VLANs, deve haver um processo de roteamento . Em cada VLAN, há um domínio de broadcast diferente. As portas de VLANs diferentes ficam isoladas pelo switch e a tabela MAC possui um índice que indica qual VLAN pertence a cada MAC. Devido ao potencial grande número de VLANs, os roteadores possuem uma funcionalidade de interfaces virtuais que são identificadas pelo VID de cada VLAN. Esta configuração tem o nome de *Router-on-a-stick* que é o uso de interfaces virtuais de rede para cada uma das VLANs. A interface física do roteador é conectada a uma porta em modo tronco no switch. São configuradas interfaces no roteador com um endereço IP em cada VLAN, sendo que este endereço específico terá a função de *gateway* em cada VLAN participante da porta tronco.

Fisicamente, a conexão da interface do roteador é limitada pela velocidade da porta, por exemplo em uma porta 1 Gbit/s todas as VLANs farão roteamento compartilhando esta interface. É possível usar interfaces físicas para realizar os roteamento entre VLANs, a limitação é a quantidade de interfaces físicas do roteador. Uma das formas de melhorar o desempenho do roteamento entre múltiplas VLANs é com o uso de um switch *layer 3* (camada 3). A funcionalidade de roteamento possibilita que o *backplane* do switch, sem a limitação da largura de banda de uma porta física, faça o encaminhamento dos pacotes, melhorando o desempenho no roteamento entre VLANs.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

4.6 Estudo de Caso: Empresa ACME

A empresa Acme está distribuída em um prédio de 8 andares, sendo cada um dos andares com necessidades de conectividade distintas. A arquitetura de rede da Acme foi projetada para garantir eficiência, segurança e escalabilidade, fazendo uso extensivo de VLANs para segmentar o tráfego e otimizar o uso dos recursos de rede. A empresa, atualmente, possui 300 colaboradores que ficam distribuídos pelos 8 andares. O total de dispositivos (computadores e notebooks) conectados em rede totalizam 350 unidades. Ainda existem 12 impressoras, 45 telefones IPs, 36 APs, além de 48 câmeras IP. A empresa possui 15 servidores hospedados no data center. Foram adquiridos switches Huawei modelo S5720 de 48 portas para serem utilizados no projeto. Na Figura 27, um diagrama simplificado com o cenário de VLANs da empresa Acme.

Figura 27. Cenário simplificado de VLANs da empresa Acme

Para atender aos seus diversos serviços e otimizar o gerenciamento, a Acme implementou a estrutura de VLANs que está na Tabela 31.

Tabela 31. Estrutura de VLANs da empresa Acme

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

VLAN ID	Descrição	Endereçamento IP
101 a 108	**VLANs de Usuários**. Uma VLAN dedicada para cada andar, segregando os dispositivos de usuários finais	Andar 1 (VLAN 101): 192.168.101.0/24 Andar 2 (VLAN 102): 192.168.102.0/24 Andar 3 (VLAN 103): 192.168.103.0/24 Andar 4 (VLAN 104): 192.168.104.0/24 Andar 5 (VLAN 105): 192.168.105.0/24 Andar 6 (VLAN 106): 192.168.106.0/24 Andar 7 (VLAN 107): 192.168.107.0/24 Andar 8 (VLAN 108): 192.168.108.0/24
1	**VLAN de Gerenciamento**. Essencial para o acesso remoto e a configuração de todos os dispositivos de rede, garantindo uma camada de segurança e controle	192.168.1.0/24
10	**VLAN de Impressoras**. Agrupa todas as impressoras da empresa, facilitando o gerenciamento e a aplicação de políticas de acesso	192.168.10.0/24
11	**VLAN de Câmeras de Vigilância**. Dedicada aos dispositivos de vigilância IP, garantindo a largura de banda e a segurança necessárias para o monitoramento	192.168.11.0/24
12	**VLAN de Telefonia IP**. Separa o tráfego de voz, priorizando-o para garantir a qualidade das chamadas e evitar interrupções	192.168.12.0/24
3	**VLAN do Data Center**. Exclusiva para os servidores e equipamentos do data center, oferecendo um ambiente seguro e de alta performance	192.168.3.0/24
2	**VLAN de Gerenciamento Wireless**. Usada para a comunicação entre os Access Points (APs) e a controladora wireless	192.168.2.0/24
13	**VLAN de Dados Wireless**. Para o tráfego de dados dos usuários conectados à rede sem fio	192.168.13.0/24

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

A infraestrutura de rede da Acme segue um modelo hierárquico, otimizado para a expansão e o desempenho que totalizam 42 switches (32 de acesso, 8 de distribuição e 2 de *core*:

- **Data Center**: Localizado no data center, dois switches *core* centralizam toda a comunicação da rede. São usados dois switches para haver redundância em caso de uma falha.
- **Conectividade por Andar**: Em cada um dos 8 andares, há um switch de distribuição que se conecta diretamente ao switch *core*, formando o *backbone* da rede.
- **Acesso de Usuários**: Cada switch de distribuição em um andar se conecta a quatro switches de acesso, totalizando 32 switches de acesso no prédio (4 por andar e 8 andares). Estes switches são o ponto de conexão final para os dispositivos de usuários, impressoras, câmeras e telefones IP.
- **Servidores Dedicados**: Os servidores de VoIP, câmeras e impressoras são projetados com duas interfaces físicas. Uma interface é dedicada à vlan do data center (vlan 3) para gerenciamento e acesso a serviços internos de data center, e a outra interface é conectada à vlan específica do serviço (vlan 12 para VoIP, vlan 11 para câmeras, vlan 10 para impressoras), garantindo a segmentação e o tráfego otimizado. Os demais servidores ficam na VLAN 3 do data center.
- **Roteamento Inter-VLAN e Acesso à Internet**: Um roteador Linux, com uma única interface física em 10 Gbit/s conectada ao switch *core* através de uma porta **trunk**, é o responsável pelo roteamento entre todas as VLANs e pelo provimento de acesso à Internet.

Em cada andar existem câmeras de vigilância, rede sem fios, impressoras e telefonia VoIP, além da respectiva VLAN do andar. Por exemplo, no primeiro andar, o switch de distribuição deverá ter configurado as VLANs 101, 1, 2, 10, 11, 12, 13 na porta *trunk* com o switch *core*. Os *uplinks* para os switches de acesso, que são 4 em cada andar, poderão ter todas estas VLANs ou algumas VLANs não serão necessárias. Um exemplo seria a não configuração da VLAN de Telefonia IP em um *uplink* com um switch de acesso que não possui um dispositivo de Telefonia IP conectado. Na Figura 28, um diagrama com as conexões dos uplinks entre os switches de distribuição dos andares com o switch *core*, onde cada switch de distribuição conecta-se ao switch *core* e aos quatro switches de acesso do seu respectivo andar.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

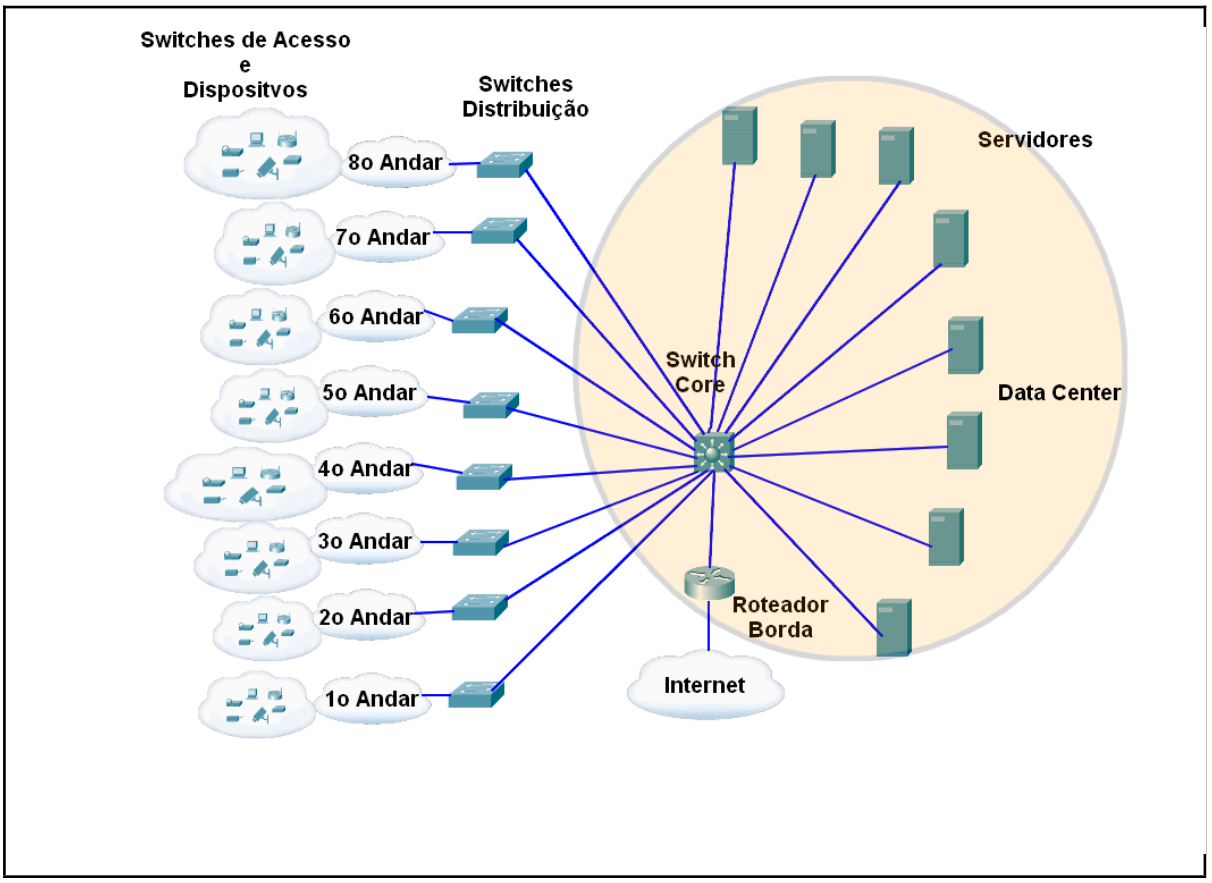


Figura 28. Diagrama com as conexões entre os switches de distribuição e o switch core.

Na Tabela 32 estão as configurações básicas de VLANs nos switches. O switch core possui funcionalidades de layer 3, sendo o responsável por fazer o roteamento entre as VLANs. Em caso de acesso a redes externas, o switch *core* tem configurado o endereço da interface do roteador de borda Linux que possui conexão com à Internet.

Tabela 32. Configurações básicas des VLANs

Switch	***Configuração***
Core	*<switch>system-view* *[switch]sysname Core_Switch* *[Core_Switch]vlan batch 1 2 3 10 11 12 13 101 to 108 // Criação de todas as VLANs* *[Core_Switch]interface Vlanif1* *[Core_Switch]ip address 192.168.1.254 255.255.255.0 // IP de gerenciamento do switch core* *[Core_Switch]interface Vlanif3* *[Core_Switch]ip address 192.168.3.1 255.255.255.0 // Gateway para a VLAN do Data Center* *[Core_Switch]interface Vlanif10*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

	[Core_Switch]ip address 192.168.10.1 255.255.255.0 // Gateway para a VLAN de Impressoras *[Core_Switch]interface Vlanif11* *[Core_Switch]ip address 192.168.11.1 255.255.255.0 // Gateway para a VLAN de Câmeras* *[Core_Switch]interface Vlanif12* *[Core_Switch]ip address 192.168.12.1 255.255.255.0 // Gateway para a VLAN de Telefonia IP* *[Core_Switch]interface Vlanif13* *[Core_Switch]ip address 192.168.13.1 255.255.255.0 // Gateway para a VLAN de Dados Wireless* *[Core_Switch]interface Vlanif2* *[Core_Switch]ip address 192.168.2.1 255.255.255.0 // Gateway para a VLAN de Gerenciamento Wireless* *// Configuração das VLANs de usuários (exemplo para VLAN 101, mesmo comando para as outras VLANs de 102 a 108)* *[Core_Switch]interface Vlanif101* *[Core_Switch]ip address 192.168.101.1 255.255.255.0 // Gateway para VLAN 101* *// Configuração das portas para os switches de distribuição (Trunk)* *// Exemplo: GigabitEthernet0/0/1 para o switch de distribuição do Andar 1* *[Core_Switch]interface GigabitEthernet0/0/1* *[Core_Switch]description Uplink Distribuicao - Andar 1* *[Core_Switch]port link-type trunk* *[Core_Switch]port trunk allow-pass vlan all* *[Core_Switch]port trunk pvid vlan 1 // VLAN nativa para gerenciamento* *// Configuração da porta para o Roteador Linux (Acesso)* *[Core_Switch]interface GigabitEthernet0/0/9* *[Core_Switch]description Roteador Linux* *[Core_Switch]port link-type access* *// Configuração das portas para os servidores (exemplo: servidor de VoIP). Esta configuração será similar para os outros servidores que possuem VLANs associadas (Impressoras, Câmeras, Wireless)* *// Servidor VoIP: Uma interface na VLAN 3 (Data Center), outra na VLAN 12 (Telefonia IP)* *[Core_Switch]interface GigabitEthernet0/0/10* *[Core_Switch]description VoIP Server - DC* *[Core_Switch]port link-type access* *[Core_Switch]port default vlan 3* *[Core_Switch]interface GigabitEthernet0/0/11* *[Core_Switch]description VoIP Server - VoIP*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

	[Core_Switch]port link-type access *[Core_Switch]port default vlan 12* *// Configura o gateway padrão para o roteador Linux* *[Huawei] ip route-static 0.0.0.0 0.0.0.0 192.168.3.254*
Distribuição	*Exemplo para o switch de distribuição do Andar 1. A configuração é similar para os outros switches de distribuição dos andares.* *<switch>system-view* *[switch]sysname Dist_Switch_Andar_1* *[Dist_Switch_Andar_1]vlan batch 1 2 3 10 11 12 13 101 // Apenas as VLANs relevantes para o andar e serviços compartilhados* *[Dist_Switch_Andar_1]interface Vlanif1* *[Dist_Switch_Andar_1]ip address 192.168.1.101 255.255.255.0 // IP de gerenciamento do switch de distribuição do Andar 1* *[Dist_Switch_Andar_1]ip route-static 0.0.0.0 0.0.0.0 192.168.1.254 // Rota padrão para o Core Switch* *// Configuração da porta para o switch core (Trunk)* *[Dist_Switch_Andar_1]interface GigabitEthernet0/0/1* *[Dist_Switch_Andar_1]description Uplink - Core* *[Dist_Switch_Andar_1]port link-type trunk* *[Dist_Switch_Andar_1]port trunk allow-pass vlan all* *[Dist_Switch_Andar_1]port trunk pvid vlan 1* *// Configuração das portas para os switches de acesso (Trunk)* *// Exemplo: GigabitEthernet0/0/2 para o switch de acesso 1 do Andar 1* *[Dist_Switch_Andar_1]interface GigabitEthernet0/0/2* *[Dist_Switch_Andar_1]description Uplink - Switch 1 - Andar 1* *[Dist_Switch_Andar_1]port link-type trunk* *[Dist_Switch_Andar_1]port trunk allow-pass vlan 1 2 10 11 12 13 101 // Permite apenas as VLANs relevantes para o andar e serviços* *[Dist_Switch_Andar_1]port trunk pvid vlan 1*
Acesso	*Exemplo para um switch de acesso no Andar 1 (Switch 1 - Andar 1):* *<switch>system-view* *[switch]sysname Access_Switch_1_Andar_1* *[Access_Switch_1_Andar_1]vlan batch 1 2 10 11 12 13 101 // VLANs relevantes para este switch de acesso* *[Access_Switch_1_Andar_1]interface Vlanif1* *[Access_Switch_1_Andar_1]ip address 192.168.1.151 255.255.255.0 // IP de gerenciamento do switch de acesso (Ex: 192.168.1.151 a 192.168.1.154 para o*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

	Andar 1) *[Access_Switch_1_Andar_1]ip route-static 0.0.0.0 0.0.0.0 192.168.1.101 // Rota padrão para o Switch de Distribuição do Andar 1* *// Configuração da porta para o switch de distribuição (Trunk)* *[Access_Switch_1_Andar_1]interface GigabitEthernet0/0/1* *[Access_Switch_1_Andar_1]description Uplink - Distribuicao - Andar 1* *[Access_Switch_1_Andar_1]port link-type trunk* *[Access_Switch_1_Andar_1]port trunk allow-pass vlan 1 2 10 11 12 13 101* *[Access_Switch_1_Andar_1]port trunk pvid vlan 1* *// Configuração das portas de acesso para dispositivos de usuários (VLAN 101)* *// Exemplo: GigabitEthernet0/0/2 a GigabitEthernet0/0/10 (aqui pode ser usado o comando:* ***interface range gigabitethernet 0/0/2 to gigabitethernet 0/0/10*** *para aplicar a VLAN em um conjunto de portas)* *[Access_Switch_1_Andar_1]interface GigabitEthernet0/0/2* *[Access_Switch_1_Andar_1]description Dispositivo - VLAN 101* *[Access_Switch_1_Andar_1]port link-type access* *[Access_Switch_1_Andar_1]port default vlan 101* *// Configuração de portas para Telefones IP (Voice VLAN - VID 12, Data VLAN - VID 101)* *// Um telefone IP geralmente marca (tagged) o tráfego de voz e passa o tráfego de dados para o PC conectado como não marcado (untagged)* *[Access_Switch_1_Andar_1]interface GigabitEthernet0/0/11* *[Access_Switch_1_Andar_1]description Telefone IP - Dados VLAN 101, Voz VLAN 12* *[Access_Switch_1_Andar_1]port link-type hybrid* *[Access_Switch_1_Andar_1]port hybrid untagged vlan 101 // Dados dos usuários (PC atrás do telefone)* *[Access_Switch_1_Andar_1]port hybrid tagged vlan 12 // Voz do telefone* *[Access_Switch_1_Andar_1]voice-vlan 12 enable* *// Configuração de portas para Câmeras de Vigilância (VLAN 11)* *[Access_Switch_1_Andar_1]interface GigabitEthernet0/0/12* *[Access_Switch_1_Andar_1]description Camera IP - VLAN 11* *[Access_Switch_1_Andar_1]port link-type access* *[Access_Switch_1_Andar_1]port default vlan 11* *// Configuração de portas para Impressoras (VLAN 10)* *[Access_Switch_1_Andar_1]interface GigabitEthernet0/0/13* *[Access_Switch_1_Andar_1]description Impressora - VLAN 10* *[Access_Switch_1_Andar_1]port link-type access* *[Access_Switch_1_Andar_1]port default vlan 10*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

	// Configuração de portas para Access Points (Trunk) *// A controladora wireless usa VLAN 2, e os dados dos usuários wireless usam VLAN 13* *[Access_Switch_1_Andar_1]interface GigabitEthernet0/0/14* *[Access_Switch_1_Andar_1]description AP - Data VLAN 13, Mgmt VLAN 2* *[Access_Switch_1_Andar_1]port link-type trunk* *[Access_Switch_1_Andar_1]port trunk allow-pass vlan 2 13* *[Access_Switch_1_Andar_1]port trunk pvid vlan 2 // PVID para a VLAN de gerenciamento do AP*

Este estudo de caso da empresa Acme ilustra de forma abrangente o poder e a flexibilidade das VLANs em redes corporativas. Ao segmentar a rede com base em andares e tipos de serviço, demonstrou-se como a hierarquia de switches (com o switch *core* desempenhando um papel central no roteamento inter-VLAN) não só otimiza a administração, mas também impulsiona a segurança e o desempenho. A definição do escopo do endereçamento IP, alinhada ao planejamento das VLANs e ao número de dispositivos, é a base para uma infraestrutura de rede robusta e escalável, pronta para atender às demandas crescentes de qualquer organização.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

5) Configurações Avançadas

As configurações avançadas em switches são utilizadas em cenários onde a rede corporativa possui uma quantidade maior de dispositivos conectados e a administração do ambiente passa a se tornar mais complexa. O entendimento destas funcionalidades e como aplicá-las nos diferentes cenários poderá ajudar em muito a disponibilidade da rede.

Neste capítulo, a **Agregação de Portas** será detalhada como um método para aumentar a largura de banda e a tolerância a falhas. O **Espelhamento de Portas** será apresentado como uma ferramenta essencial para diagnóstico e monitoramento do tráfego. Serão apresentadas as configurações básicas do **STP (*Spanning-Tree Protocol*)** e suas variações, essencial para a prevenção de loops em topologias redundantes. Serão examinados os mecanismos de segurança como **DHCP Snooping** e **IGMP Snooping**, que protegem a rede contra ataques e otimizam o tráfego multicast, respectivamente.

A implementação de **ACLs (*Access Control Lists*)** será explorada como um método para definir políticas de segurança e controlar o acesso a recursos com base em diversos critérios. A **Limitação de Acesso em Portas** será discutida como uma medida para restringir a conexão de dispositivos não autorizados. A configuração de **QoS (*Quality of Service*)** será abordada como uma técnica para priorizar o tráfego crítico e garantir a qualidade de serviços sensíveis ao tempo. O **Monitoramento de Recursos** em switches será apresentado e tem como objetivo ajudar no diagnóstico de problemas e na melhoria do desempenho do dispositivo. A **Autenticação de Dispositivos (802.1X)** será detalhada como um padrão robusto para controlar o acesso à rede no nível da porta. Finalmente, serão exploradas as **funcionalidades de camada 3** que estão presentes em diversos modelos de switches, expandindo suas capacidades para além do *switching* tradicional e permitindo o roteamento entre VLANs e sub-redes.

5.1 Agregação de portas (*Link Aggregation*)

A agregação de portas, também conhecida como LAG (*Link Aggregation)* ou *EtherChannel* (termo popularizado pela Cisco), é uma tecnologia de rede que permite combinar múltiplas conexões físicas Ethernet em um único canal lógico. Essa agregação proporciona dois benefícios principais: aumento da largura de banda e melhoria da resiliência (tolerância a falhas).

Ao invés de utilizar uma única conexão para transmitir dados entre dois dispositivos de rede (como um switch e um servidor, ou dois switches), a agregação de portas agrupa várias interfaces físicas como se fossem uma só. O tráfego é então distribuído por meio de um algoritmo de seleção configurável entre essas interfaces físicas, permitindo que a taxa de

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

transferência agregada se aproxime da soma da capacidade individual de cada link. Como benefícios da agregação de portas podem ser citados:

- **Aumento da Largura de Banda:** Ao combinar a capacidade de múltiplas portas, a agregação de portas cria uma única interface virtual com capacidade igual ao número de portas físicas agrupadas, permitindo a transmissão de um volume maior de informações simultaneamente. Por exemplo, 4 portas físicas com capacidade de 1 Gbit/s, formam um agrupamento que terá 4 x 1 Gbit/s de capacidade, ou seja, poderiam ser trafegados 4 fluxos de 1 Gbit/s de forma simultânea se cada fluxo passar em uma interface física distinta. Isso é especialmente útil para conexões de alta demanda, como entre servidores de arquivos e a rede, ou entre switches *core* e de distribuição.

- **Melhoria da Resiliência (Tolerância a Falhas):** Se um dos links físicos que compõem o LAG falhar, o tráfego é automaticamente distribuído entre os links restantes sem interromper a conectividade. Essa redundância aumenta a confiabilidade da conexão e minimiza o tempo de inatividade da rede.

- **Balanceamento de Carga:** O tráfego é distribuído entre os membros do LAG utilizando algoritmos de balanceamento de carga. Esses algoritmos consideram diversos fatores, como endereços MAC de origem e destino, endereços IP de origem e destino e portas TCP/UDP, para garantir uma distribuição equitativa do tráfego e evitar gargalos em um único link.

Etherchannel (Link Aggregation) - https://youtu.be/rFWJB-1N99g

Embora o conceito fundamental seja o mesmo, diferentes fabricantes podem utilizar terminologias distintas para se referir à agregação de portas. Alguns termos comuns incluem:

- ***Link Aggregation* (LAG):** Termo genérico e amplamente utilizado.
- ***EtherChannel*:** Termo proprietário da Cisco.
- ***Port Trunking*:** Outro termo comum, embora às vezes possa ser confundido com o "trunking" de VLANs.
- ***Bonding*:** Termo frequentemente utilizado em sistemas operacionais de servidores para agregação de interfaces de rede.

O padrão IEEE 802.3ad, também conhecido como *Link Aggregation Control Protocol* (LACP**)**, define um método para a agregação automática de links. O LACP permite que os dispositivos negociem quais links farão parte do LAG, detectem falhas nos links e ajustem dinamicamente a participação dos links no grupo agregado. Utilizar LACP é altamente

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

recomendado, pois oferece maior flexibilidade e robustez em comparação com a agregação estática (onde os links são configurados manualmente sem negociação).

Algumas considerações de Implementação devem ser observadas:

- **Requisitos:** Para configurar um LAG, as portas a serem agregadas devem possuir a mesma velocidade, modo duplex e outras configurações relacionadas.
- **Conexão Direta:** As portas que formam um LAG devem estar conectadas diretamente entre os dois dispositivos que participam da agregação.
- **Número de Portas:** O número de portas que podem ser agregadas em um único LAG varia dependendo do equipamento, sendo a quantidade de 4 portas físicas um valor bem popular entre os switches de entrada.
- **Configuração:** A configuração da agregação de portas é realizada na interface de gerenciamento dos switches e/ou servidores envolvidos.

O uso mais comum da agregação de portas é com portas de uplink entre switches. Por exemplo, se o cascateamento entre dois switches for realizado por uma interface de 1 Gbit/s, este será o limite de tráfego que poderá ser transferido entre os dois dispositivos. Entretanto, se todas as portas dos switches tiverem a capacidade de 1 Gbit/s e entre os switches houver tráfego intenso de múltiplas portas, haverá congestionamento. Um exemplo seria se muitos computadores conectados a esses switches precisarem enviar dados ao mesmo tempo para o outro switch, essa conexão de 1 Gbit/s pode ficar congestionada.

Com o uso de agregação, o *uplink* entre os switches poderia ter 3 portas de 1 Gbit/s , possibilitando que 3 x 1 Gbit/s (3 Gbit/s agregado) fossem possíveis de serem transferidos simultaneamente. O ideal seria o uso de uma porta em 10 Gbit/s para realizar o *uplink* entre estes switches. Porém, se os switches não tiverem portas em 10 Gbit/s disponíveis o uso de agregação de portas seria a opção mais simples de realizar. Ainda haveria a opção de empilhar (*stacking*) os switches, se os modelos de switches tenham a funcionalidade de empilhamento, por meio de cabos especiais proprietários e que muitas vezes possuem custos elevados e distâncias bastante curtas para interligar os switches.

Outra vantagem importante da agregação de portas é a tolerância a falhas. Se um ou até duas portas físicas que formam a agregação falharem, a comunicação entre os switches não será totalmente interrompida, pois os cabos restantes continuarão transmitindo os dados. Na Tabela 33 estão exemplos da configuração em switches diversos.

Tabela 33. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)
** Para criar uma agregação com duas interfaces G0/1 e G0/2, com o grupo "1"* *switch>enable* *switch# conf t*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

switch(config)# interface range GigabitEthernet0/1 - 2
switch(config-if-range)# shutdown
switch(config-if-range)# channel-group 1 mode active
switch(config-if-range)# exit

switch(config)# interface Port-channel 1
switch(config-if)# description Uplink_Predio2
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk encapsulation dot1q
switch(config-if)# switchport trunk allowed vlan all
switch(config-if)# exit

switch(config)# interface range GigabitEthernet0/1 - 2
switch(config-if-range)# no shutdown
switch(config-if-range)# end
switch# show etherchannel summary

** Para remover a agregação com duas interfaces G0/1 e G0/2, com o grupo "1"*
switch>enable
switch# conf t
switch(config)# interface range GigabitEthernet0/1 - 2
switch(config-if-range)# no channel-group 1
switch(config-if-range)# exit

switch(config)# no interface Port-channel 1
switch(config)# end
switch# write memory

switch# show etherchannel summary

switch# show run interface GigabitEthernet0/1

Huawei S5720-52X-LI (CLi)

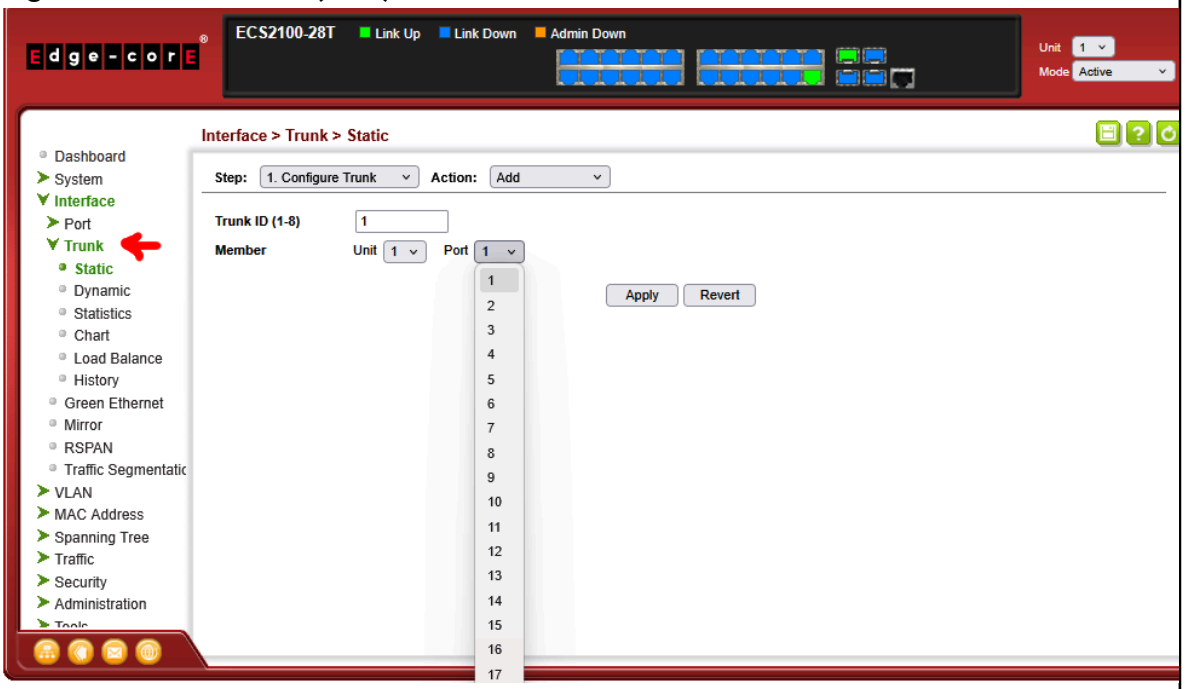
** Para criar uma agregação com duas interfaces G0/1 e G0/2, com o nome de interface Eth-Trunk 1*
<switch> system-view
[switch] interface Eth-Trunk 1
[switch-Eth-Trunk1] mode lacp-static
[switch-Eth-Trunk1] port link-type trunk
[switch-Eth-Trunk1] port trunk allow-pass vlan all
[switch-Eth-Trunk1] descriptionUplink_Predio2
[switch-Eth-Trunk1] trunkport GigabitEthernet0/0/1 to GigabitEthernet0/0/2
[switch-Eth-Trunk1] quit
[switch] save

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

<switch> display eth-trunk 1

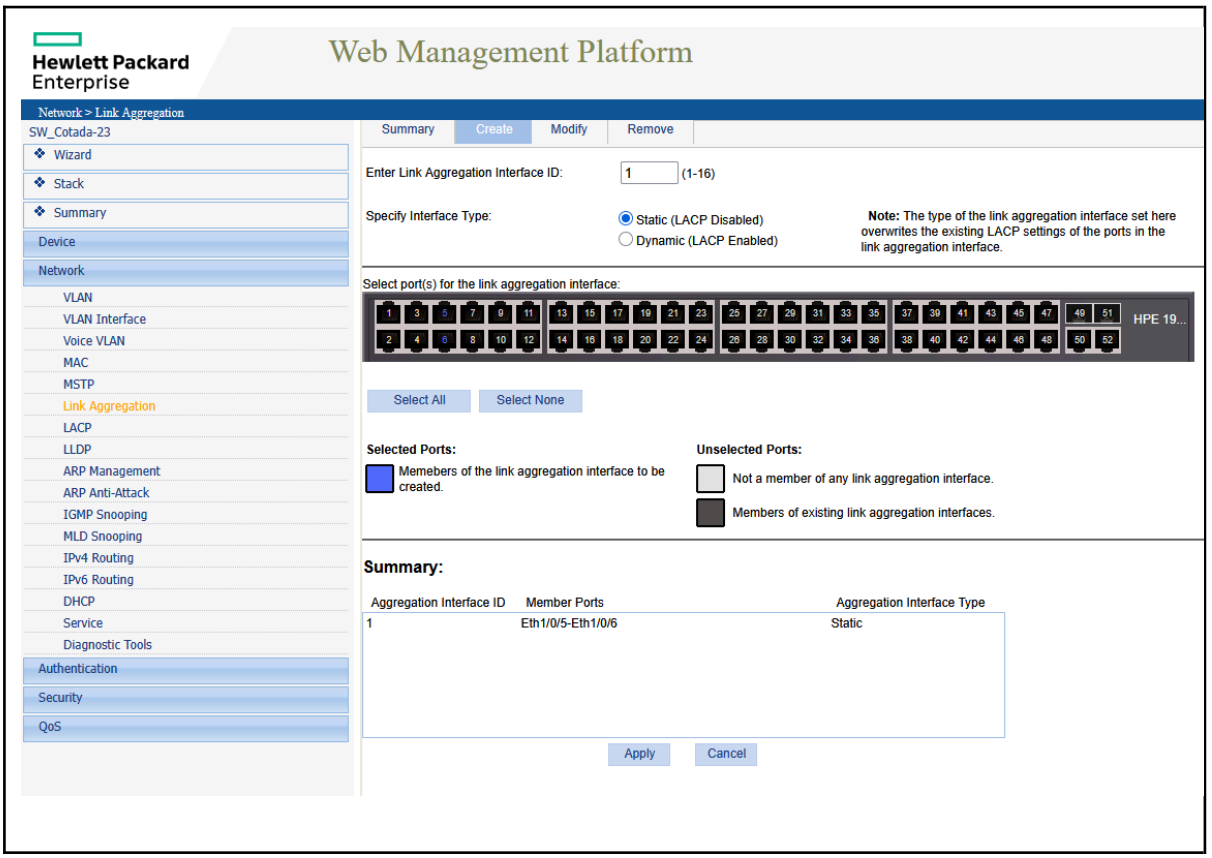
** Para remover uma agregação com duas interfaces G0/1 e G0/2, com o nome de interface Eth-Trunk 1*
<switch> system-view
[switch] undo interface Eth-Trunk 1

Edgecore ECS2100-28T (Web)



HP 1910-48 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



5.2 Espelhamento de Portas (*Port MIrroring*/SPAN)

O espelhamento de portas, também conhecido como *Port Mirroring* ou SPAN (*Switched Port Analyzer*), é uma funcionalidade que permite copiar o tráfego de rede que entra ou sai de uma ou mais portas de origem (*source ports*) para uma porta de destino específica (*destination port*). Essa cópia do tráfego é então utilizada para análise, diagnóstico e monitoramento sem interferir no fluxo normal de dados da rede. Por exemplo, a porta de *uplink* com o roteador de borda pode ser usada por uma ferramenta de NIDS (*Network Intrusion Detection System*) para detectar anomalias e ataques no tráfego com a Internet.

Ao configurar o espelhamento de portas, o switch replica os pacotes que passam pelas portas de origem e os envia para a porta de destino. Um dispositivo de análise conectado à porta de destino pode então capturar e examinar esse tráfego duplicado. É importante notar que a porta de destino geralmente é dedicada à função de espelhamento e o tráfego enviado para ela pelo dispositivo de análise não é transmitido para outras portas do switch. Os tipos de modos para espelhamento de portas são:

- **SPAN (*Local SPAN*):** O tráfego é espelhado de uma ou mais portas de origem para uma porta de destino localizada no mesmo switch. Este é o tipo mais comum de espelhamento de portas.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **RSPAN (*Remote SPAN*)*:** Permite espelhar o tráfego de portas de origem em um switch para uma porta de destino em um switch diferente. Isso geralmente envolve a utilização de VLANs especiais (RSPAN VLANs) para transportar o tráfego espelhado através da rede.

- **ERSPAN (*Encapsulated Remote SPAN*)*:** Uma evolução do RSPAN que encapsula o tráfego espelhado utilizando um cabeçalho GRE (*Generic Routing Encapsulation*). Isso permite o espelhamento de tráfego através de redes roteadas (Layer 3), oferecendo maior flexibilidade em topologias complexas.

** Nos casos onde é realizado o espelhamento remoto, RSPAN e ERSPAN, deve-se considerar o volume de tráfego que será transmitido entre as portas de uplinks dos switches, onde o volume gerado de pacotes poderá causar congestionamento.*

As aplicações mais comuns do espelhamento de portas são na análise de tráfego de rede em conjunto com ferramentas de segurança para detecção de anomalias e ataques, tais como:

- **Análise de Tráfego:** Permite capturar e analisar o tráfego de rede utilizando ferramentas como analisadores de tráfego (Wireshark, tcpdump) ou *probes* de Netflow para entender padrões de comunicação, identificar gargalos, diagnosticar problemas de desempenho e monitorar a utilização da largura de banda.

- **Detecção e Prevenção de Intrusão (IDS/IPS):** O tráfego espelhado pode ser enviado para sistemas de detecção e prevenção de intrusão para identificar atividades maliciosas e tentativas de acesso não autorizado à rede.

- **Monitoramento de Segurança:** Ajuda a monitorar o tráfego em busca de atividades suspeitas, como a propagação de malware, comunicação com servidores de comando e controle, e tentativas de exploração de vulnerabilidades.

- **Diagnóstico de Problemas:** Ao capturar o tráfego em pontos específicos da rede onde ocorrem problemas, por exemplo na porta de um dispositivo cliente, é possível analisar os pacotes para identificar a causa raiz de falhas de conectividade, erros de comunicação ou problemas de aplicação.

- **Monitoramento de VoIP:** Permite gravar e analisar chamadas VoIP para fins de qualidade de serviço, *troubleshooting* ou conformidade regulatória.

- **Conformidade e Auditoria:** O tráfego espelhado pode ser utilizado para fins de auditoria e conformidade, registrando as comunicações de rede para análise

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

posterior.

Wireshark Tutorial - Dicas - Capturas em Cenários -

https://www.youtube.com/watch?v=KXJ6L2Q1mTA

Ao ser realizada a configuração do espelhamento de portas deve-se levar em consideração alguns fatores importantes:

- **Impacto no Desempenho:** O espelhamento de portas pode consumir recursos do switch, especialmente em redes com alto volume de tráfego. É importante monitorar o consumo de cpu do switch após a configuração do espelhamento.

- **Capacidade da Porta de Destino:** A porta de destino deve ter capacidade suficiente para lidar com o volume de tráfego espelhado das portas de origem. Em alguns casos, pode ser necessário utilizar uma porta com maior largura de banda. Por exemplo, espelhar 2 portas com capacidade de 1 Gbit/s em uma porta de 10Gbit/s.

- **Configuração:** A configuração do espelhamento de portas é realizada na interface de gerenciamento do switch, especificando as portas de origem (podendo ser uma ou várias, e em ambas as direções - entrada e saída) e a porta de destino.

- **Limitações:** Alguns switches podem ter limitações no número de sessões de espelhamento que podem ser configuradas simultaneamente ou no tipo de tráfego que pode ser espelhado.

Na Tabela 34 estão exemplos da configuração em switches diversos.

Tabela 34. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)
** Espelhamento das portas G0/1 e G0/3 na porta G0/2* *switch>enable* *switch# configure terminal* *switch(config)# monitor session 1 destination interface GigabitEthernet0/2* *switch(config)# monitor session 1 source interface GigabitEthernet0/1* *switch(config)# monitor session 1 source interface GigabitEthernet0/3* *switch(config)# end*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

switch# show monitor session 1

** Para remover a sessão de espelhamento de número 1*
switch(config)# no monitor session 1

Huawei S5720-52X-LI (CLi)

** Para criar um espelhamento das portas G0/0/1 e G0/0/3 na porta G0/0/2*
<switch> system-view
[switch] observe-port GigabitEthernet0/0/2

[switch] interface GigabitEthernet0/0/1
[switch-GigabitEthernet0/0/1] port-mirroring to observe-port GigabitEthernet0/0/2 inbound
[switch-GigabitEthernet0/0/1] port-mirroring to observe-port GigabitEthernet0/0/2 outbound

[switch] interface GigabitEthernet0/0/3
[switch-GigabitEthernet0/0/1] port-mirroring to observe-port GigabitEthernet0/0/3 inbound
[switch-GigabitEthernet0/0/1] port-mirroring to observe-port GigabitEthernet0/0/3 outbound

<switch> display port-mirroring

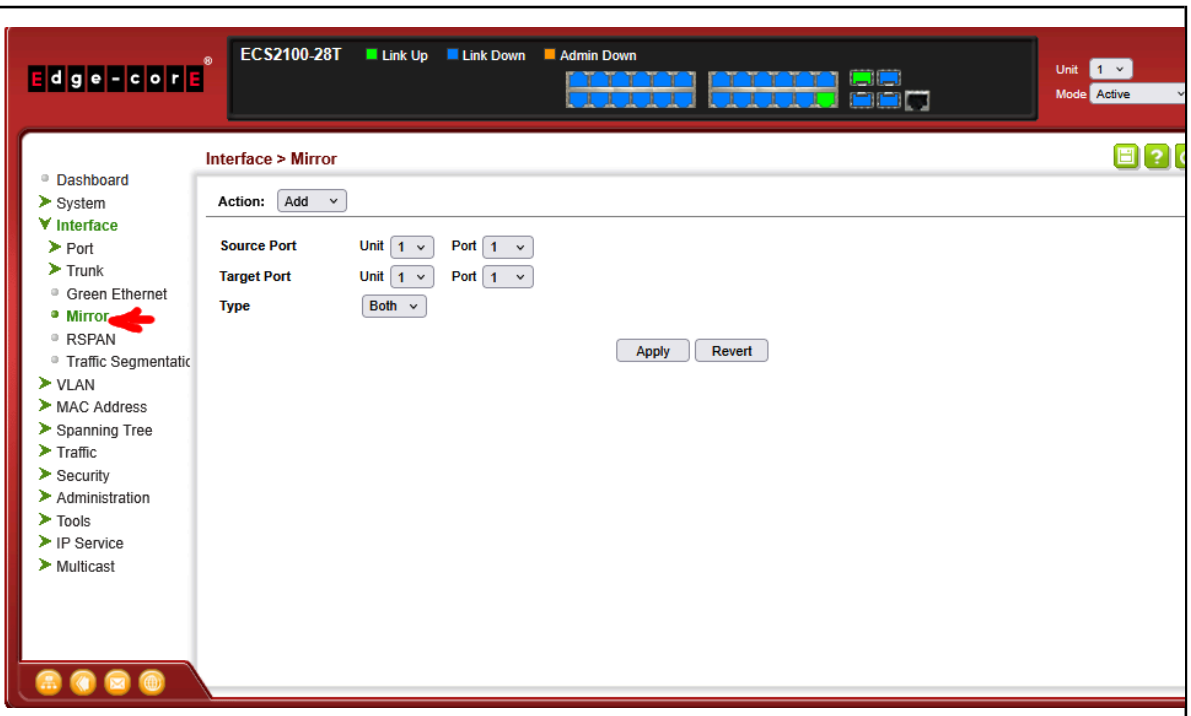
** Para remover o espelhamento das portas G0/0/1 e G0/0/3 na porta G0/0/2*
[switch] interface GigabitEthernet0/0/1
[switch-GigabitEthernet0/0/1] undo port-mirroring to observe-port G0/0/2 inbound
[switch-GigabitEthernet0/0/1] undo port-mirroring to observe-port G0/0/2 outbound
[switch-GigabitEthernet0/0/1] quit

[switch] interface GigabitEthernet0/0/3
[switch-GigabitEthernet0/0/3] undo port-mirroring to observe-port G0/0/2 inbound
[switch-GigabitEthernet0/0/3] undo port-mirroring to observe-port G0/0/2 outbound
[switch-GigabitEthernet0/0/3] quit

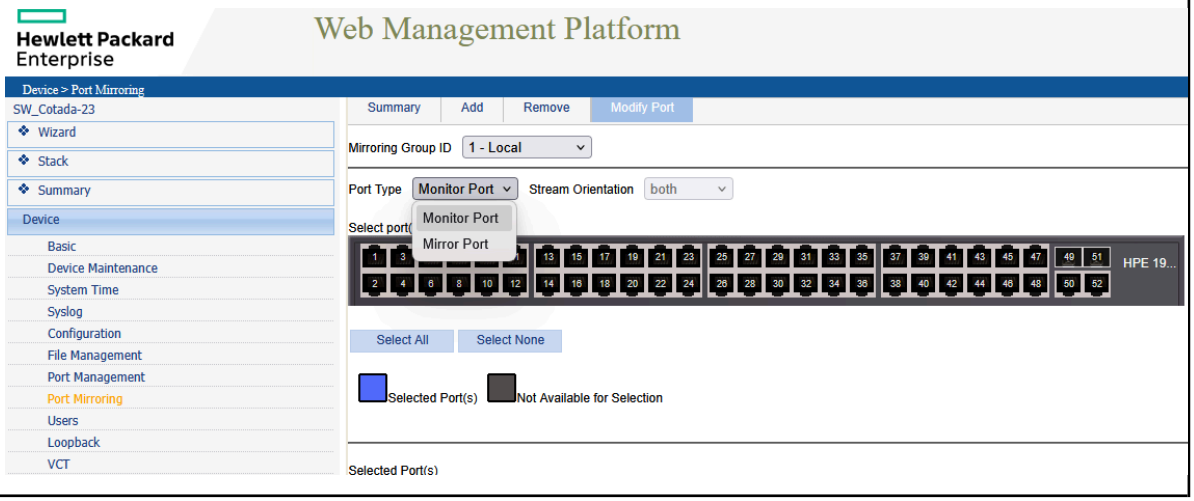
[switch] undo observe-port GigabitEthernet0/0/2

Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



HP 1910-48 (Web)



5.3 STP (*Spanning-Tree Protocol*)

O STP (*Spanning-Tree Protocol*) é um protocolo de camada 2, camada de Enlace de Dados, definido pelo padrão IEEE 802.1D. Sua principal função é prevenir a formação de *loops* de encaminhamento em redes Ethernet que possuem múltiplas rotas entre switches. A presença de *loops* pode levar a problemas graves como tempestades de broadcast, duplicação de quadros e instabilidade da rede, tornando a comunicação degradada. Outra

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

funcionalidade é possibilitar o uso de enlaces redundantes entre switches, onde um caminho poderá assumir a conexão em caso de indisponibilidade da conexão que estava em uso.

Loop na Rede - https://youtu.be/rLuZiuNkB7A

Em topologias de rede com redundância (múltiplos caminhos entre switches), é possível que ocorram *loops*. Isso pode acontecer devido a configurações incorretas ou para garantir a disponibilidade da rede em caso de falha de um link. No entanto, sem um mecanismo de controle, esses loops podem causar:

- **Tempestades de Broadcast:** Um quadro de broadcast enviado em um *loop* será repassado indefinidamente pela rede, sendo replicado por cada switch e consumindo toda a largura de banda disponível.
- **Duplicação de Quadros:** Os mesmos quadros podem chegar ao destino várias vezes, causando confusão e erros nas aplicações.
- **Instabilidade da Tabela MAC:** Os switches aprendem endereços MAC associando-os às portas por onde os quadros chegam. Em um *loop*, um mesmo endereço MAC pode ser aprendido em diferentes portas repetidamente, tornando a tabela MAC instável e prejudicando o encaminhamento correto.

O STP resolve o problema de *loops* criando uma topologia lógica em forma de árvore, desativando (bloqueando) algumas das rotas redundantes. O protocolo realiza isso através dos seguintes passos:

1. **Eleição do *Root Bridge* (Ponte Raiz):** Todos os switches na rede participam de um processo de eleição para determinar um único switch como a Ponte Raiz (*Root Bridge*). A Ponte Raiz é o ponto central da topologia STP. A eleição é baseada em um valor de prioridade configurável e no endereço MAC do switch (o switch com a menor prioridade ou, em caso de empate, o menor endereço MAC é eleito).

2. **Determinação do *Root Port* (Porta Raiz):** Cada switch não raíz identifica uma única porta como sua *Root Port*. Esta é a porta com o menor custo de caminho (*path cost*) até a Ponte Raiz. O custo do caminho é uma métrica associada a cada link, geralmente baseado na velocidade da porta (links mais rápidos têm menor custo).

3. **Seleção das *Designated Ports* (Portas Designadas):** Em cada segmento de rede (link entre dois switches ou entre um switch e um dispositivo final), uma porta é eleita como *Designated Port*. Esta é a porta no segmento com o menor custo de caminho até a Ponte Raiz. A *Designated Port* é responsável por encaminhar o tráfego para aquele segmento.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

4. **Bloqueio de Portas:** Todas as portas que não são *Root Ports* ou *Designated Ports* são colocadas em estado de bloqueio (*blocking*). Portas bloqueadas não encaminham tráfego de dados, evitando assim a formação de *loops*. Elas continuam ouvindo as BPDUs (*Bridge Protocol Data Units*), que são mensagens de controle do STP, para se manterem atualizadas sobre a topologia da rede.

As portas STP passam por diferentes estados durante o processo de convergência e operação:

- ***Blocking*:** A porta não encaminha tráfego de dados e não aprende endereços MAC. Ela apenas ouve as BPDUs.
- ***Listening*:** A porta está ouvindo as BPDUs e participando da eleição da Ponte Raiz e das portas designadas, mas ainda não vai encaminhar tráfego ou aprender endereços MAC.
- ***Learning*:** A porta ainda não encaminha tráfego, mas começa a aprender os endereços MAC dos dispositivos conectados ao segmento.
- ***Forwarding*:** A porta encaminha tráfego de dados e aprende endereços MAC. Este é o estado operacional normal para as *Root Ports* e *Designated Ports*.
- ***Disabled*:** A porta está administrativamente desativada e não participa do STP.

Os switches se comunicam entre si utilizando BPDUs (*Bridge Protocol Data Units*). Essas mensagens contêm informações sobre a Ponte Raiz, o custo do caminho e as IDs dos switches e portas envolvidas. As BPDUs são trocadas regularmente para manter a topologia STP atualizada e para detectar mudanças na rede (por exemplo, falha de um link). Na Figura 29, um exemplo de um pacote do tipo BPDU capturado no Wireshark.

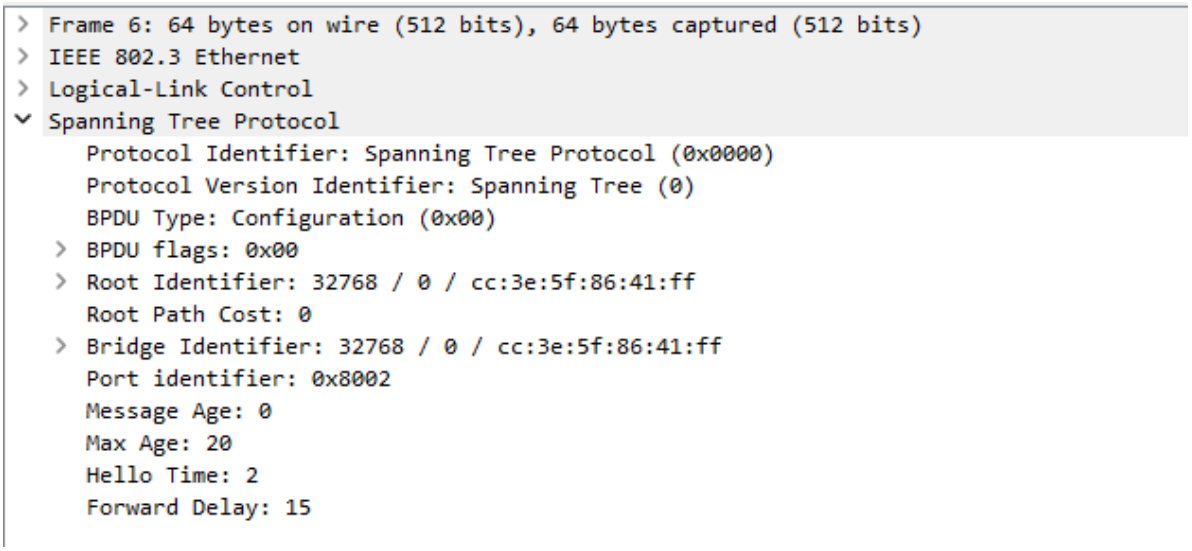


Figura 29. Exemplo de pacote BPDU

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Ao longo do tempo, o STP evoluiu para versões mais rápidas e eficientes, como:

- **RSTP (*Rapid Spanning-Tree Protocol*) - IEEE 802.1w:** Oferece uma convergência muito mais rápida em comparação com o STP original.
- **MSTP (*Multiple Spanning-Tree Protocol*) - IEEE 802.1s:** Permite criar múltiplas instâncias de STP, onde cada instância pode gerenciar a topologia de uma ou mais VLANs, otimizando o uso dos links redundantes.

O STP é um protocolo fundamental para garantir a estabilidade e a confiabilidade de redes Ethernet com redundância, como no caso de topologias em anel ou em *mesh*. Sem ele, a presença de *loops* poderia rapidamente levar a uma falha generalizada da rede. Entretanto, o uso de STP para limitar *loops* na rede depende se todos os switches possuem o protocolo ativado.

Por exemplo, se houver um *loop* em um switch sem STP ou da funcionalidade de *Loop Protection*, o *loop* afetará parte da rede. No caso que este switch sem STP estiver conectado com dois *uplinks* a um switch com STP ativado uma das portas será bloqueada. Entretanto, se o *loop* for em portas no switch sem STP, o *loop* será repassado para a porta de *uplink* no switch com STP ativado. Os dispositivos que estiverem conectados ao switch sem STP serão afetados pelo efeito do *loop*. A correta compreensão e configuração do STP (ou suas versões mais recentes) são essenciais para qualquer administrador de redes. Na Tabela 35 estão exemplos da configuração em switches diversos.

Tabela 35. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

```
switch>enable

* Porta de usuário, com convergência rápida e filtro para pacotes BPDU
switch# configure terminal
switch(config)# interface GigabitEthernet0/1
switch(config-if)# spanning-tree portfast
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# end

* Define um custo STP menor, padrão em interfaces gigabit seria 2000, na interface para
encaminhar os pacotes de acordo com o interesse do administrador
switch# configure terminal
switch(config)# interface GigabitEthernet0/23
switch(config-if)# spanning-tree cost 1000
switch(config-if)# end

* Para obter informações sobre a execução do STP
switch#show spanning-tree
```

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

switch#show spanning-tree summary
switch#show spanning-tree interface GigabitEthernet0/1 detail

**Nos switches Cisco modelo 2960 o protocolo STP está ativado por padrão em todas as portas.*

Huawei S5720-52X-LI (CLi)

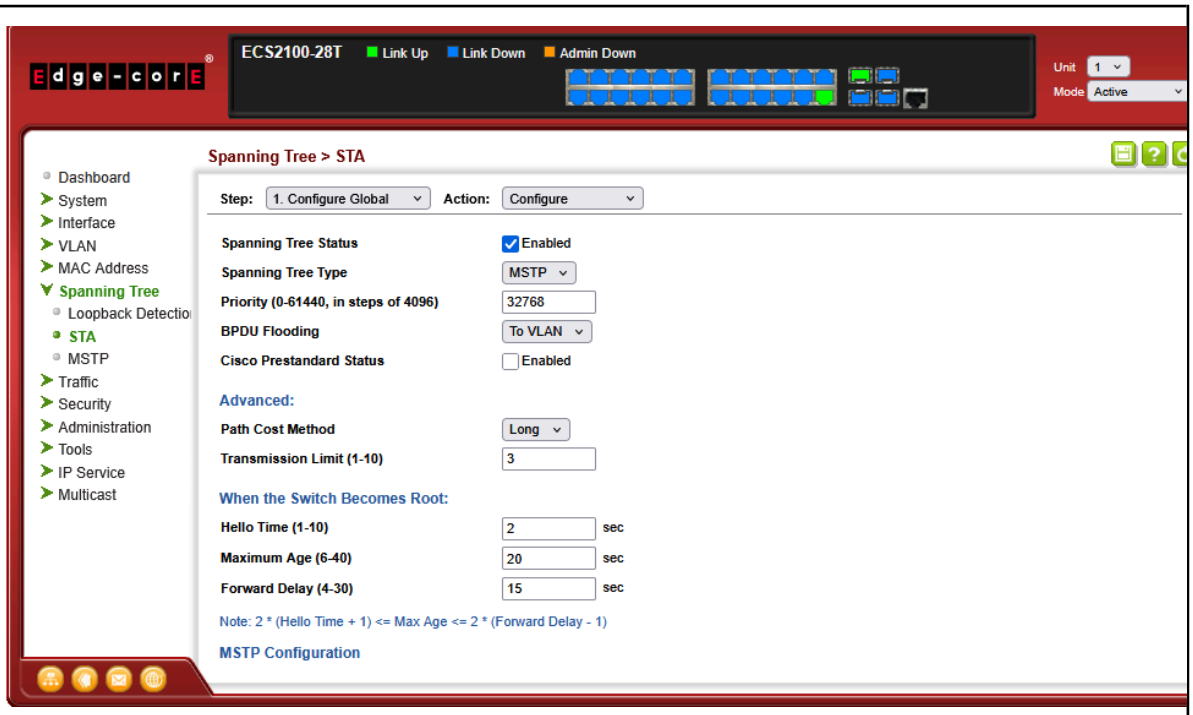
** Porta de usuário, com convergência rápida e filtro para pacotes BPDU*
<switch> system-view
[switch] interface GigabitEthernet0/0/1
[switch-GigabitEthernet0/0/1] stp edged-port enable
[switch-GigabitEthernet0/0/1] bpdu-protection
[switch-GigabitEthernet0/0/1] quit

** Define um custo STP menor, padrão em interfaces gigabit seria 2000, na interface para encaminhar os pacotes de acordo com o interesse do administrador*
<switch> system-view
[switch] interface GigabitEthernet0/0/23
[switch-GigabitEthernet0/0/23] stp cost 1000
[switch-GigabitEthernet0/0/23] quit

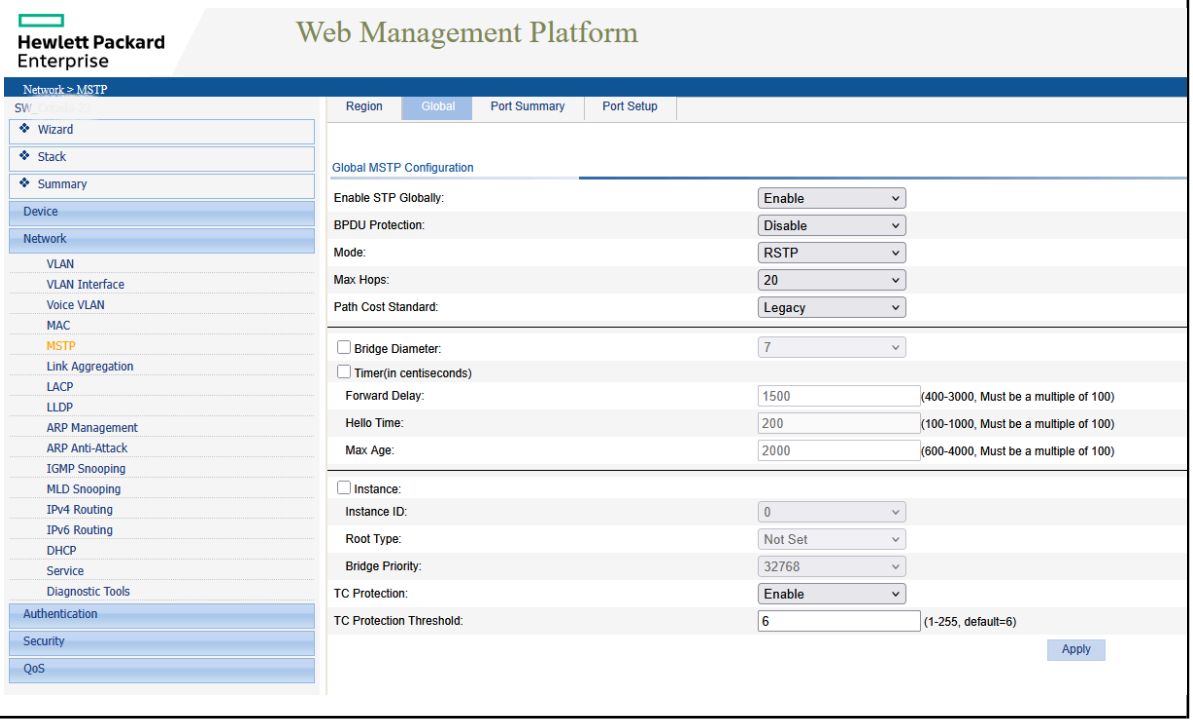
** Para obter informações sobre a execução do STP*
<switch>display stp
<switch>display stp brief
<switch>display stp interface GigabitEthernet0/0/1

Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



HP 1910-48 (Web)



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

5.4 DHCP Snooping

O *DHCP Snooping* é um recurso de segurança para mitigar ataques baseados no protocolo DHCP (*Dynamic Host Configuration Protocol*). Esta funcionalidade atua controlando quais servidores DHCP são considerados confiáveis e filtrando mensagens DHCP maliciosas que poderiam ser utilizadas para comprometer a rede.

DHCP Snooping - evitando DHCP indesejado na rede - https://youtu.be/WjutKkBziFI

Em uma rede local, os clientes DHCP enviam solicitações (*DHCP Discover*) para obter informações de configuração de rede, como endereço IP, máscara de sub-rede, gateway padrão e servidores DNS. Servidores DHCP autorizados respondem com ofertas (*DHCP Offer*), e o cliente escolhe uma oferta e envia uma solicitação (*DHCP Request*) para confirmar a alocação. Finalmente, o servidor DHCP envia um reconhecimento (*DHCP ACK*) com as informações de configuração. O problema surge quando servidores DHCP não autorizados (*rogue DHCP servers*) são introduzidos na rede. Esses servidores podem fornecer informações de configuração incorretas ou maliciosas aos clientes, permitindo ataques como:

- **Negação de Serviço (DoS):** Fornecendo endereços IP inválidos ou conflitantes, impedindo que os clientes se comuniquem na rede.
- ***Man-in-the-Middle*:** Fornecendo o endereço IP de um atacante como *gateway* padrão ou servidor DNS, permitindo que o tráfego seja interceptado e manipulado.

O *DHCP Snooping* funciona construindo e mantendo uma tabela de ligação DHCP Snooping denominada *DHCP Snooping Binding Table*. Esta tabela contém informações sobre os endereços MAC dos clientes, os endereços IP atribuídos a eles, o tempo de concessão do *lease* DHCP e a porta do switch na qual o cliente recebeu a concessão. Para construir e manter essa tabela, o *DHCP Snooping* classifica as portas do switch em duas categorias:

- **Portas Confiáveis (*Trusted Ports*):** Portas que estão conectadas a servidores DHCP legítimos e controlados pela administração da rede. O tráfego DHCP vindo dessas portas é considerado válido e é encaminhado normalmente.

- **Portas Não Confiáveis (*Untrusted Ports*):** Portas que estão conectadas a *hosts* finais (clientes), outros switches não controlados ou qualquer dispositivo onde um servidor DHCP não autorizado possa ser conectado. O tráfego DHCP vindo dessas portas é inspecionado e certas mensagens podem ser descartadas.

O *DHCP Snooping* implementa os seguintes mecanismos de filtragem para proteger a rede:

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Bloqueio de Mensagens DHCP Server de Portas Não Confiáveis:** A principal função do *DHCP Snooping* é impedir que mensagens *DHCP Offer*, *DHCP ACK* e *DHCP Lease Query* originadas de portas não confiáveis alcancem os clientes. Apenas mensagens *DHCP Offer* e *DHCP ACK* recebidas em portas confiáveis são encaminhadas aos clientes.

- **Validação do Endereço MAC e do Endereço IP:** O *DHCP Snooping* pode validar se o endereço MAC do cliente na mensagem *DHCP Request* corresponde ao endereço MAC de origem do pacote Ethernet. Além disso, alguns switches podem verificar se o endereço IP atribuído pelo servidor DHCP corresponde à entrada na tabela de ligação *DHCP Snooping* para evitar respostas falsificadas.

- **Limitação da Taxa de Mensagens DHCP:** Para prevenir ataques de exaustão de DHCP (*DHCP starvation attacks*), onde um atacante inunda o servidor DHCP com inúmeras solicitações para esgotar seus endereços IP disponíveis, o *DHCP Snooping* pode limitar a taxa de mensagens *DHCP Request* que são aceitas em portas não confiáveis.

No processo de aprendizagem da tabela de ligação, a tabela de ligação *DHCP Snooping* é populada da seguinte forma:

1. Um cliente DHCP envia uma mensagem *DHCP Discover*.
2. Um servidor DHCP confiável responde com uma mensagem *DHCP Offe*r através de uma porta confiável.
3. O cliente envia uma mensagem *DHCP Request* através de uma porta não confiável.
4. O switch com *DHCP Snooping* habilitado intercepta a mensagem *DHCP Request*.
5. Se a mensagem for válida (de acordo com as políticas configuradas), o switch encaminha a solicitação ao servidor DHCP através de uma porta confiável.
6. O servidor DHCP responde com uma mensagem *DHCP ACK* através de uma porta confiável.
7. O switch intercepta a mensagem *DHCP ACK* e cria uma entrada na tabela de ligação *DHCP Snooping*, associando o endereço MAC do cliente, o endereço IP atribuído, o tempo de concessão e a porta não confiável pela qual o cliente enviou a solicitação.
8. O switch então encaminha a mensagem *DHCP ACK* ao cliente através da porta não confiável.

A configuração do *DHCP Snooping* geralmente envolve os seguintes passos:

1. **Habilitar o DHCP Snooping globalmente** no switch.
2. **Habilitar o DHCP Snooping em VLANs específicas** onde a proteção é necessária.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

3. **Definir as portas confiáveis.** Geralmente, as portas conectadas a servidores DHCP controlados e outros switches da rede são configuradas como confiáveis. Todas as outras portas de acesso são consideradas não confiáveis por padrão.

O *DHCP Snooping* é uma funcionalidade essencial na administração de redes locais evitando que servidores de DHCP não autorizados causem ataques e indisponibilidade nos dispositivos de rede. Sem isto, o administrador terá muitas dificuldades para identificar a origem do servidor de DHCP não autorizado e para retornar a normalidade da rede nos dispositivos que receberem configurações de endereçamento errados. Na Tabela 36 estão exemplos da configuração em switches diversos.

Tabela 36. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)
switch> enable *switch# configure terminal* ** Ativa o DHCP Snooping de forma global, todas as portas passam para o estado de Untrust* *switch(config)# ip dhcp snooping* ** Ativa o DHCP Snooping somente nas VLANs 10, 20, e 30 (todas as portas nestas VLANs ficam como Untrust)* *switch(config)# ip dhcp snooping vlan 10,20,30* ** Porta G0/24 será confiável para pacotes de servidores de DHCP* *switch(config)# interface GigabitEthernet0/24* *switch(config-if)# ip dhcp snooping trust* *switch(config-if)# exit* ** Exibe o status global do DHCP Snooping e as VLANs habilitadas* *switch#show ip dhcp snooping* ** Exibe a tabela de bindings DHCP (IP, MAC, VLAN, porta, tempo de lease)* *switch#show ip dhcp snooping binding* ** Exibe estatísticas de pacotes DHCP snooping, incluindo pacotes descartados* *switch#show ip dhcp snooping statistics* ** Exibe quais interfaces são configuradas como confiáveis* *switch#show ip dhcp snooping trust*
Huawei S5720-52X-LI (CLi)
<switch> system-view ** Ativa o DHCP Snooping de forma global, todas as portas passam para o estado de Untrust* *[switch] dhcp snooping enable*

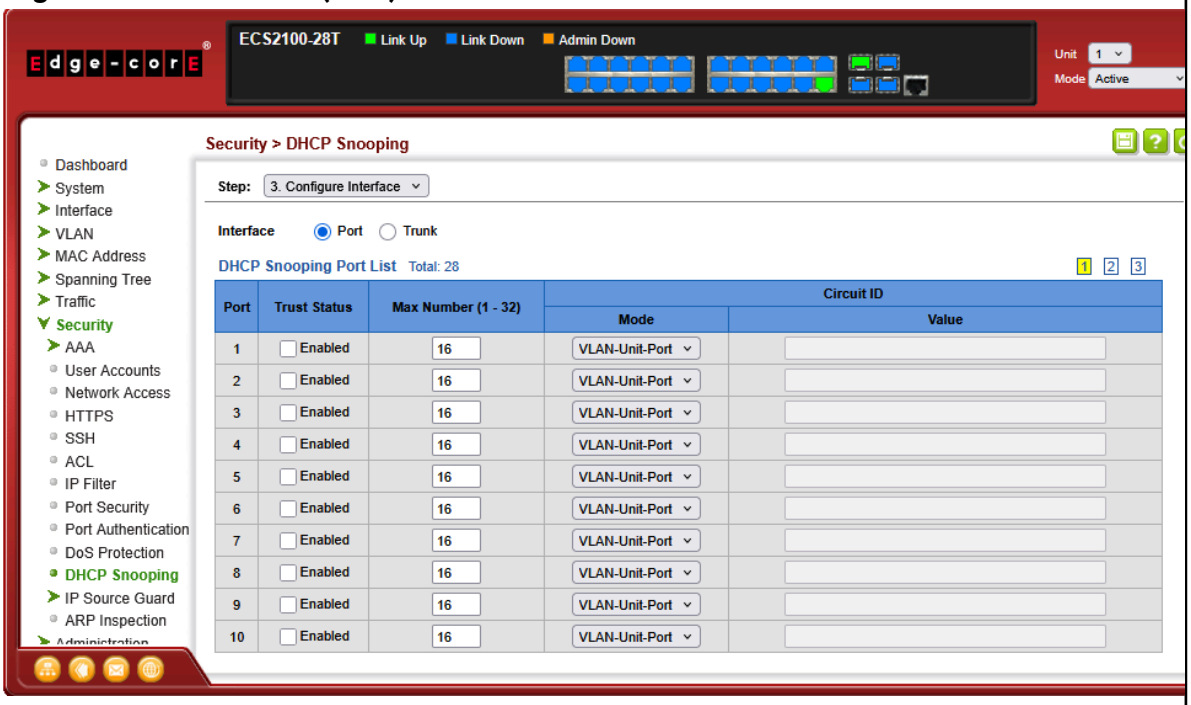
Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

** Ativa o DHCP Snooping somente nas VLANs 10, 20, e 30 (todas as portas nestas VLANs ficam como Untrust)*
[switch] vlan 10
[switch-vlan10] dhcp snooping enable
[switch-vlan10] quit
[switch] vlan 20
[switch-vlan20] dhcp snooping enable
[switch-vlan20] quit

** Porta G0/24 será confiável para pacotes de servidores de DHCP*
[switch] interface GigabitEthernet0/0/24
[switch-GigabitEthernet0/0/24] dhcp snooping trusted
[switch-GigabitEthernet0/0/24] quit

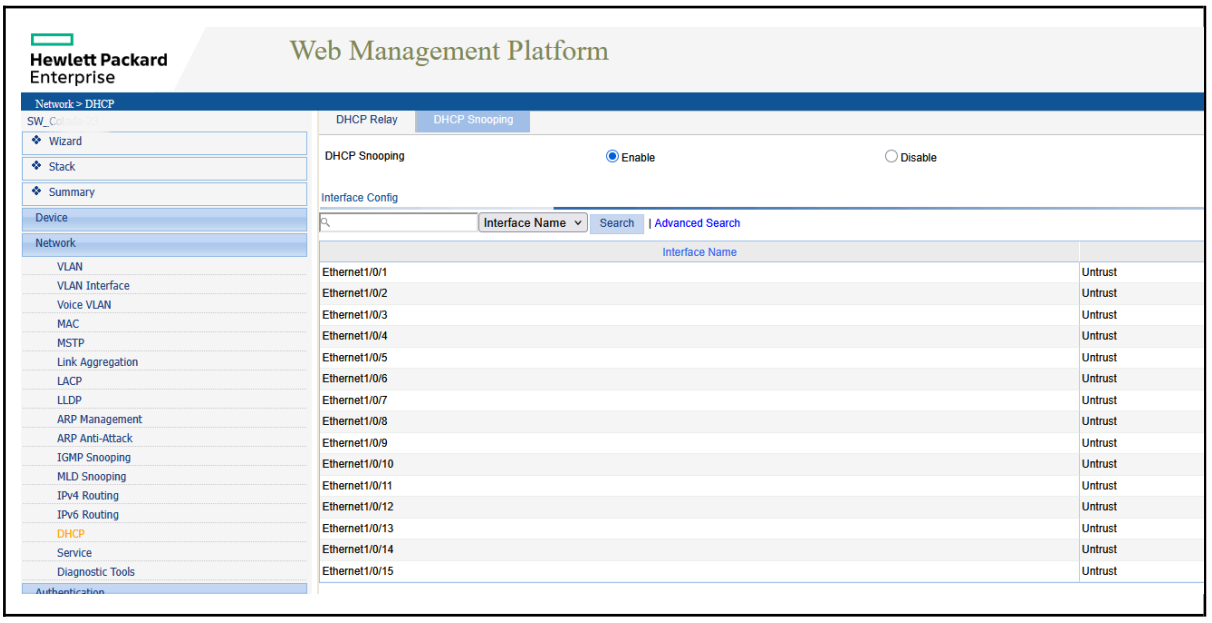
** Exibe o status global do DHCP Snooping e as VLANs habilitadas*
<switch> display dhcp snooping
** Exibe a tabela de bindings DHCP (IP, MAC, VLAN, porta, tempo de lease)*
<switch> display dhcp snooping binding:
** Exibe o status DHCP Snooping de uma interface específica*
<switch> display dhcp snooping interface GigabitEthernet0/0/1

Edgecore ECS2100-28T (Web)



HP 1910-48 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



5.5 IGMP Snooping

O *IGMP Snooping* é uma funcionalidade que otimiza a entrega de tráfego multicast em uma rede local Ethernet. A transmissão em multicast é usada quando há necessidade de envio de dados para serviços de forma seletiva, utilizado para descoberta de serviços ou para troca de dados em serviços específicos.

São usados endereços nas camadas de enlace de dados e de rede que identificam um grupo de multicast, formado por hosts que compartilham de um mesmo endereço em comum. Os endereços MAC com prefixo **01:00:5E:XX:XX:XX** com os 3 primeiros bytes são usados para identificar que é uma transmissão multicast e os últimos 3 bytes são usados para identificar o grupo de multicast. Na camada de rede, em IPv4 a Classe D 224.0.0.0 – 239.255.255.255 serve para identificar o grupo. Por exemplo, o endereço IPv4 224.0.100.10 pode ser usado por todos os hosts que participam de um mesmo grupo de multicast. Este endereço é convertido na camada de enlace para o MAC 01-00-5e-00-64-0a. A conversão de IPv4 de multicast para o endereço MAC correspondente pode ser feito usando a ferramenta de conversão disponível em https://www.dqnetworks.ie/toolsinfo.d/multicastaddressing.html.

Em IPv6 todos os endereços que começam com “ff” são para multicast e existem vários grupos específicos, por exemplo ff02::1 que representa um grupo com todos os hosts na rede. Na RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks, disponível em https://datatracker.ietf.org/doc/html/rfc2464 explica o método de conversão do endereço IPv6 multicast para um endereço MAC que é basicamente a concatenação do prefixo **33-33** com os últimos 32 bits do endereço IPv6 multicast. Um exemplo seria o endereço IPv6 de multicast ff02::16 que teria o endereço MAC correspondente 33-33-00-00-00-16. Em IPv6

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

não há o protocolo IGMP e a funcionalidade similar é o MLD (*Multicast Listener Discovery*) *Snooping*.

Redes para Iniciantes - Tipos de Transmissão -
https://www.youtube.com/watch?v=Rk_B5v5LC2g

Transmissão de streaming com VLC (multicast) -
https://www.youtube.com/watch?v=ptoBYEV7p_w

Sem o *IGMP Snooping*, o tráfego multicast é tratado como tráfego em broadcast e encaminhado para todas as portas do switch, mesmo para aquelas onde não há hosts interessados em receber esse tráfego, desperdiçando largura de banda e potencialmente sobrecarregando os dispositivos finais.

Quando um host deseja receber um fluxo de tráfego multicast (por exemplo, uma transmissão de vídeo), ele envia mensagens IGMP *(Internet Group Management Protocol*) para informar aos roteadores multicast sobre seu interesse em um grupo específico. No entanto, switches de camada 2 tradicionais não inspecionam essas mensagens IGMP. Eles simplesmente veem o tráfego multicast chegando em uma porta e o encaminham para todas as outras portas da mesma VLAN (*Virtual Local Area Network)*, como se fosse um broadcast. Isso causa os seguintes problemas:

- **Desperdício de Largura de Banda:** Hosts que não estão interessados recebem o tráfego multicast, consumindo largura de banda desnecessariamente.
- **Sobrecarga de Dispositivos Finais:** Dispositivos que recebem tráfego multicast não solicitado precisam processá-lo e descartá-lo, consumindo recursos de CPU e memória.
- **Ineficiência da Rede:** A rede se torna menos eficiente, especialmente em ambientes com grande quantidade de tráfego multicast, como *streaming* de vídeo, IPTV ou videoconferências.

O *IGMP Snooping* permite que o switch "espione" (snoop) as mensagens IGMP trocadas entre os hosts e os roteadores multicast. Ao analisar essas mensagens, o switch aprende em quais portas têm hosts interessados em receber tráfego para grupos multicast específicos. Com base nessa informação, o switch cria tabelas de encaminhamento multicast que mapeiam grupos multicast para as portas relevantes. Quando o switch recebe tráfego multicast para um determinado grupo, ele encaminha esse tráfego apenas para as portas que

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

possuem hosts registrados para esse grupo, evitando a inundação desnecessária de outras portas.

Ao permitir que os switches interpretem as mensagens IGMP, isto garante que o tráfego multicast seja entregue apenas aos destinatários pretendidos, otimizando a largura de banda e melhorando o desempenho geral da rede. Na Tabela 37 estão exemplos da configuração em switches diversos.

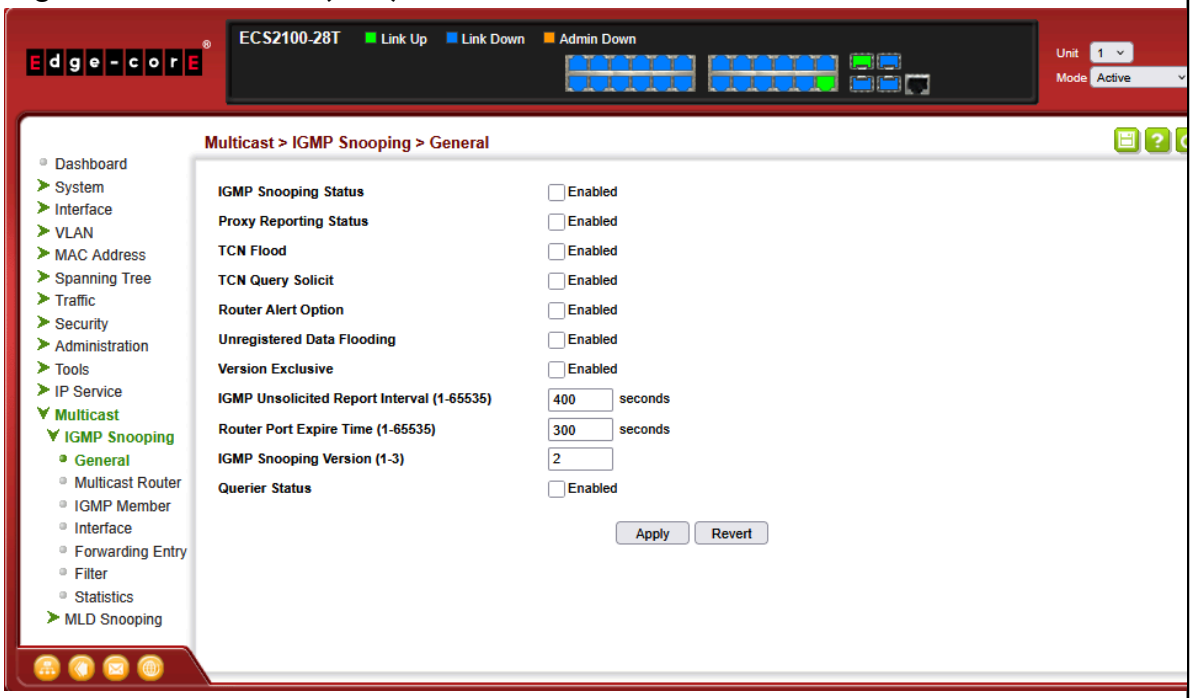
Tabela 37. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch#conf t* ** Ativa o IGMP Snooping de forma global* *switch(config)# ip igmp snooping* *switch(config)# ip igmp snooping querier* ** Ativa o IGMP Snooping na VLAN 10* *switch(config)# interface vlan 10* *switch(config-if)#ip igmp snooping* *switch(config-if)# ip igmp snooping querier* *switch(config-if)# end* ** Exibe o status global do IGMP Snooping e das VLANs onde ele está habilitado* *switch#show ip igmp snooping* ** Exibe detalhes do IGMP Snooping para uma VLAN específica, incluindo o querier e os membros do grupo* *switch#show ip igmp snooping vlan [vlan_id]* ** Exibe todos os grupos multicast aprendidos pelo IGMP Snooping e as portas associadas* *switch#show ip igmp snooping groups*
Huawei S5720-52X-LI (CLi) *<switch> display-view* ** Ativa o IGMP Snooping de forma global* *[switch] igmp-snooping enable* ** Ativa o IGMP Snooping na VLAN 10* *[switch] vlan 10* *[switch-vlan10] igmp-snooping enable* *[switch-vlan10] igmp-snooping querier enable* *[switch-vlan10] quit* ** Exibe o status global do IGMP Snooping* *display igmp-snooping global* ** Exibe detalhes do IGMP Snooping para uma VLAN específica*

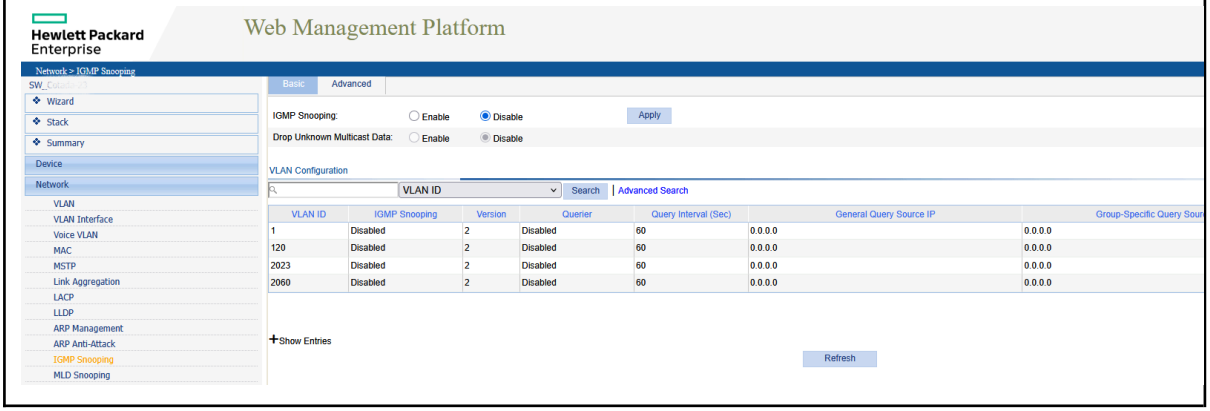
Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

display igmp-snooping vlan [vlan_id]
** Exibe informações do IGMP Snooping para uma interface específica*
display igmp-snooping port [interface_type interface_number]
** Exibe todos os grupos multicast aprendidos e as portas associadas*
display igmp-snooping group

Edgecore ECS2100-28T (Web)



HP 1910-48 (Web)



5.6 Loop Detection

O protocolo de *Loop Detection* (Detecção de Loop) é um mecanismo essencial em switches gerenciáveis para prevenir a formação de *loops*. Esses *loops* podem ocorrer devido a configurações incorretas, falhas de hardware ou topologias redundantes mal

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

implementadas. Os *loops* causam a duplicação e transmissão contínua de pacotes, levando a uma tempestade de broadcast, alto consumo de largura de banda e, eventualmente, a paralisação da rede.

O *Loop Detection* funciona monitorando continuamente as interfaces do switch em busca de pacotes de controle específicos enviados pelo próprio switch. A ideia principal é que, se um switch receber um pacote de controle que ele mesmo enviou de volta por outra interface, isso indica a presença de um *loop*.

As principais funcionalidades do Loop Detection são:

- **Envio de Pacotes de Controle**: O switch envia periodicamente pacotes de controle especiais (muitas vezes chamados de BPDUs (*Bridge Protocol Data Units*), embora com uma finalidade diferente do STP/RSTP) por todas as interfaces habilitadas para *Loop Detection*. Esses pacotes contêm informações de identificação do switch e da interface de origem.
- **Monitoramento das Interfaces:** Cada interface habilitada para *Loop Detection* monitora o tráfego recebido em busca desses pacotes de controle específicos.
- **Detecção de Loop**: Se uma interface receber um pacote de controle que tenha a mesma identificação do **próprio switch como origem**, isso significa que o pacote viajou por um caminho em *loop* e retornou.
- **Ação de Bloqueio**: Ao detectar um *loop*, o switch toma uma ação para interrompê-lo. A ação mais comum é desabilitar (bloquear) a interface que recebeu o pacote de controle de retorno. Isso impede que o tráfego continue circulando no *loop*.
- **Recuperação**: Algumas implementações de *Loop Detection* oferecem mecanismos de recuperação automática. Periodicamente, o switch pode tentar reabilitar a interface bloqueada para verificar se o *loop* ainda existe. Se não houver mais detecção do pacote de controle de retorno, a interface é reativada. Em outros casos, a intervenção manual do administrador pode ser necessária para identificar e corrigir a causa do *loop* antes de reabilitar a porta.

Na Tabela 38 estão exemplos da configuração em switches diversos.

Tabela 38. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) ** Neste switch não há uma funcionalidade de loopback detection, apenas um proteção por meio do protocolo STP para evitar inconsistências em links redundantes*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

switch>enable
switch# configure terminal
switch(config)# interface GigabitEthernet0/1
switch(config-if)# spanning-tree loopguard enable
switch(config-if)# end

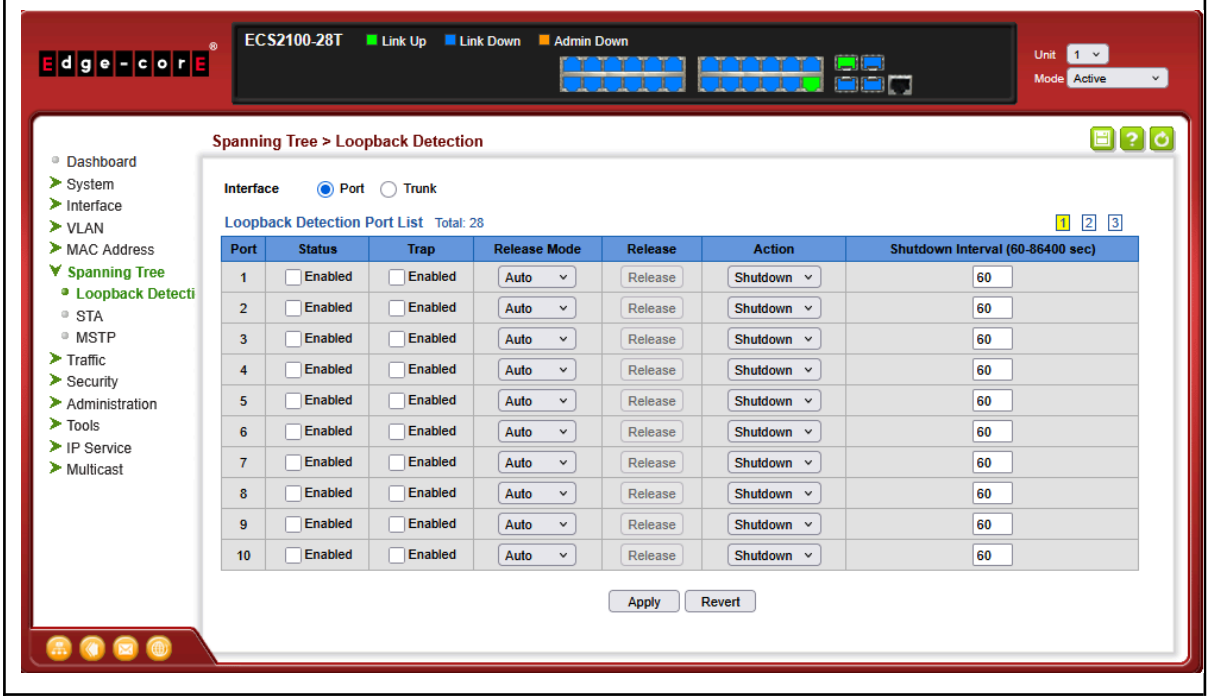
Huawei S5720-52X-LI (CLi)

** Ativa globalmente a detecção de loop*
<switch> system-view
[switch] loopback-detect enable

** Ativa a detecção em uma interface específica, G0/0/1, e ativa a ação de desabilitar a interface em caso de loop detectado*
[switch] interface GigabitEthernet0/0/1
[switch-GigabitEthernet0/0/1] loopback-detect enable
[switch-GigabitEthernet0/0/1] loopback-detect action shutdown
[switch-GigabitEthernet0/0/1] quit

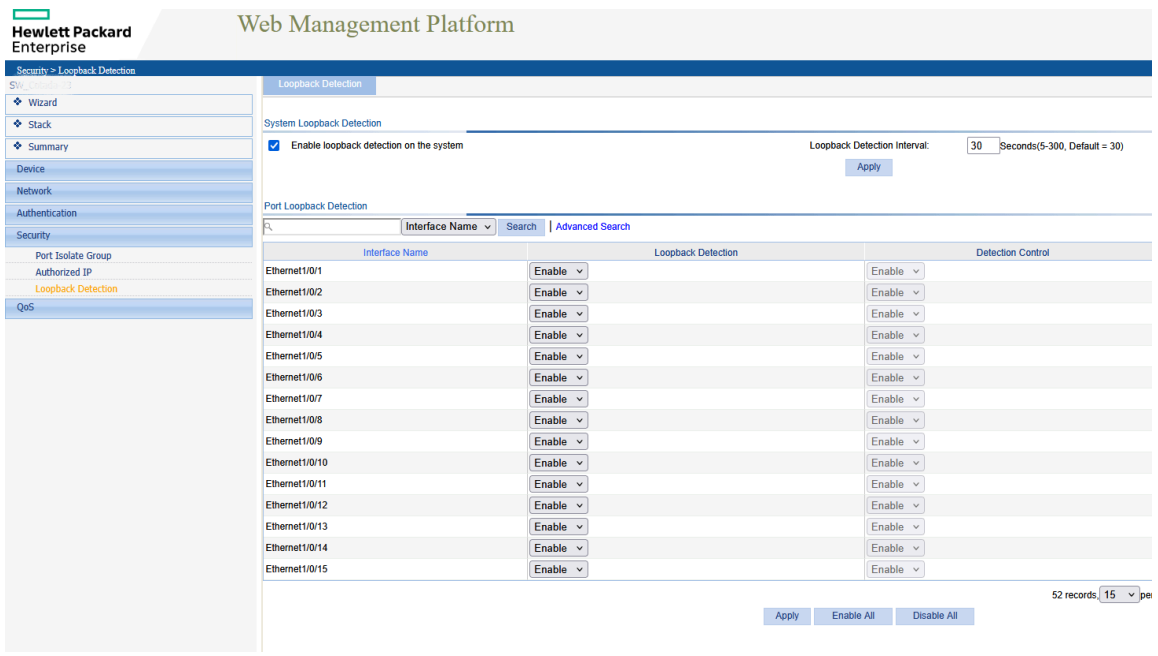
** Exibe o status global e as configurações de detecção de loop*
<switch>display loopback-detect
** Exibe o status de detecção de loop para uma interface específica*
<switch>display loopback-detect interface GigabitEthernet0/0/1

Edgecore ECS2100-28T (Web)



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

HP 1910-48 (Web)



5.7 ACL (Access Control List)

Uma **Lista de Controle de Acesso (*Access Control List* (ACL))** é um conjunto de regras configuradas que controlam o tráfego de rede com base em critérios específicos. Em switches gerenciáveis, as ACLs oferecem um mecanismo poderoso para implementar políticas de segurança, segmentar a rede e controlar o acesso a recursos, operando principalmente nas camadas 2, 3 e 4 do modelo OSI.

Uma ACL é essencialmente uma série de declarações de permissão ou negação que são avaliadas sequencialmente para cada pacote que entra ou sai de uma interface do switch. Cada declaração (ou regra) especifica as condições a serem correspondidas (por exemplo, endereço MAC ou IP de origem, endereço MAC ou IP de destino, porta TCP/UDP, protocolo) e a ação a ser tomada (permitir ou negar o tráfego). O switch processa os pacotes comparando-os com as regras da ACL na ordem em que foram definidas. A primeira regra que corresponde às características do pacote determina a ação a ser tomada (permitir ou negar). Se um pacote não corresponder a nenhuma regra específica na ACL, uma ação implícita de "negar tudo" (*deny all*) geralmente é aplicada como regra padrão no final da lista.

As ACLs em switches podem ser categorizadas com base nas informações que utilizam para filtrar o tráfego:

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **ACLs de camada 2 (MAC ACLs):** Operam na camada de enlace de dados e baseiam suas decisões de filtragem em informações do cabeçalho Ethernet, como endereços MAC de origem e destino, e o tipo de *EtherType*. São úteis para controlar o tráfego não-IP ou para aplicar controles de acesso em ambientes onde os endereços IP podem ser dinâmicos.

- **ACLs de camada 3 (IP ACLs):** Operam na camada de rede e são as mais comuns. Elas examinam informações do cabeçalho IP, como endereços IP de origem e destino, e protocolos (como ICMP, TCP, UDP).

- **ACLs de camada 4 (*Extended* ACLs):** Estendem a funcionalidade das ACLs de camada 3, permitindo a filtragem com base em informações da camada de transporte, como portas TCP e UDP de origem e destino. Isso possibilita um controle mais granular sobre aplicações específicas.

As ACLs são utilizadas para diversas funcionalidades relacionados ao tráfego de rede em switches, entre as funcionalidades mais comuns:

- **Segurança:** Controlar o acesso a recursos de rede, restringindo o tráfego entre diferentes segmentos da rede ou impedindo o acesso de hosts não autorizados.
- **Segmentação da Rede:** Implementar políticas de acesso entre VLANs, permitindo a comunicação apenas entre segmentos necessários.
- **Controle de Tráfego:** Priorizar ou limitar certos tipos de tráfego (em conjunto com QoS), ou bloquear tráfego indesejado tais como broadcasts excessivos ou ARP *flooding*.
- **Filtragem de Tráfego:** Bloquear tráfego malicioso conhecido ou tráfego baseado em protocolos específicos.
- **Implementação de Políticas de Acesso:** Garantir a conformidade com políticas de segurança corporativas.

As ACLs podem ser aplicadas às interfaces do switch em duas direções. Na direção de ***Inbound* (Entrada)** a ACL é avaliada para o tráfego que está entrando na interface do switch. As ações (permitir/negar) são tomadas antes que o tráfego seja roteado, em caso de switches com capacidade de roteamento, ou comutado para outras interfaces. Na direção de ***Outbound* (Saída)** a ACL é avaliada para o tráfego que está saindo da interface do switch. As ações são tomadas após o tráfego ter sido roteado ou comutado e antes de ser transmitido pela interface.

As ACLs são um recurso avançado para controlar o fluxo de tráfego, permitindo a implementação de políticas de segurança robustas e a otimização do desempenho da rede. Por exemplo, em caso de switches que não possuam funcionalidade em IPv6 equivalentes ao *DHCP Snooping* para IPv4 poderiam ser criadas ACLs com bloqueios para pacotes não

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

autorizados de *Router Advertisements* (RAs). Na Tabela 39 estão exemplos da configuração em switches diversos.

Tabela 39. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

switch>enable
switch#conf t
switch(config)#access-list 101 permit tcp host 192.168.1.10 host 192.168.1.100 eq 80
switch(config)#access-list 101 deny tcp any host 192.168.1.100 eq 80
switch(config)#access-list 101 permit ip any any
switch(config)#interface Vlan1
switch(config-if)# ip access-group 101 in

** Descrição dos comandos*

access-list 101 permit tcp host 192.168.1.10 host 192.168.1.100 eq 80

access-list 101: Define uma ACL estendida com número 101. Números entre 100 e 199 são para ACLs IP estendidas
permit: Permite o tráfego
tcp: Especifica o protocolo TCP
host 192.168.1.10: Define o IP de origem como o host 192.168.1.10
host 192.168.1.100: Define o IP de destino como o host 192.168.1.100
eq 80: Especifica a porta de destino como 80 (HTTP)

access-list 101 deny tcp any host 192.168.1.100 eq 80

deny: Nega o tráfego
any: Significa qualquer endereço de origem. Esta regra bloqueia qualquer outro host que tente acessar o servidor 192.168.1.100 na porta 80

access-list 101 permit ip any any

*Importante: Toda ACL tem uma **deny any any** implícita no final. Em caso de não ser adicionada a regra de **permit ip any any**, todo o tráfego restante que não for explicitamente permitido será bloqueado. Neste caso, o objetivo é bloquear apenas o acesso à porta 80 do servidor para outros hosts, mas permitir todo o resto do tráfego.*

interface Vlan1
Entra no modo de configuração da interface VLAN1 (ou a interface que seja necessário o bloqueio criado na ACL 101

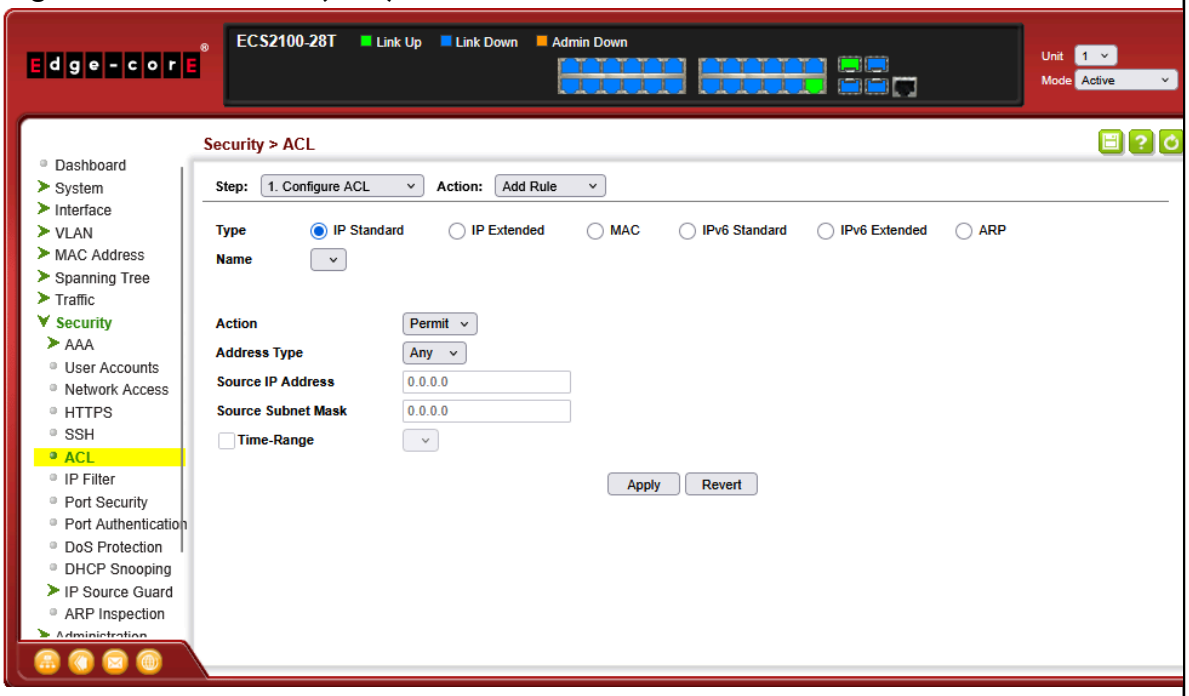
ip access-group 101 in
Aplica a ACL 101 na interface Vlan1 na direção de entrada (in). Isso significa que a ACL será aplicada ao tráfego que chega a essa interface

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Huawei S5720-52X-LI (CLi)

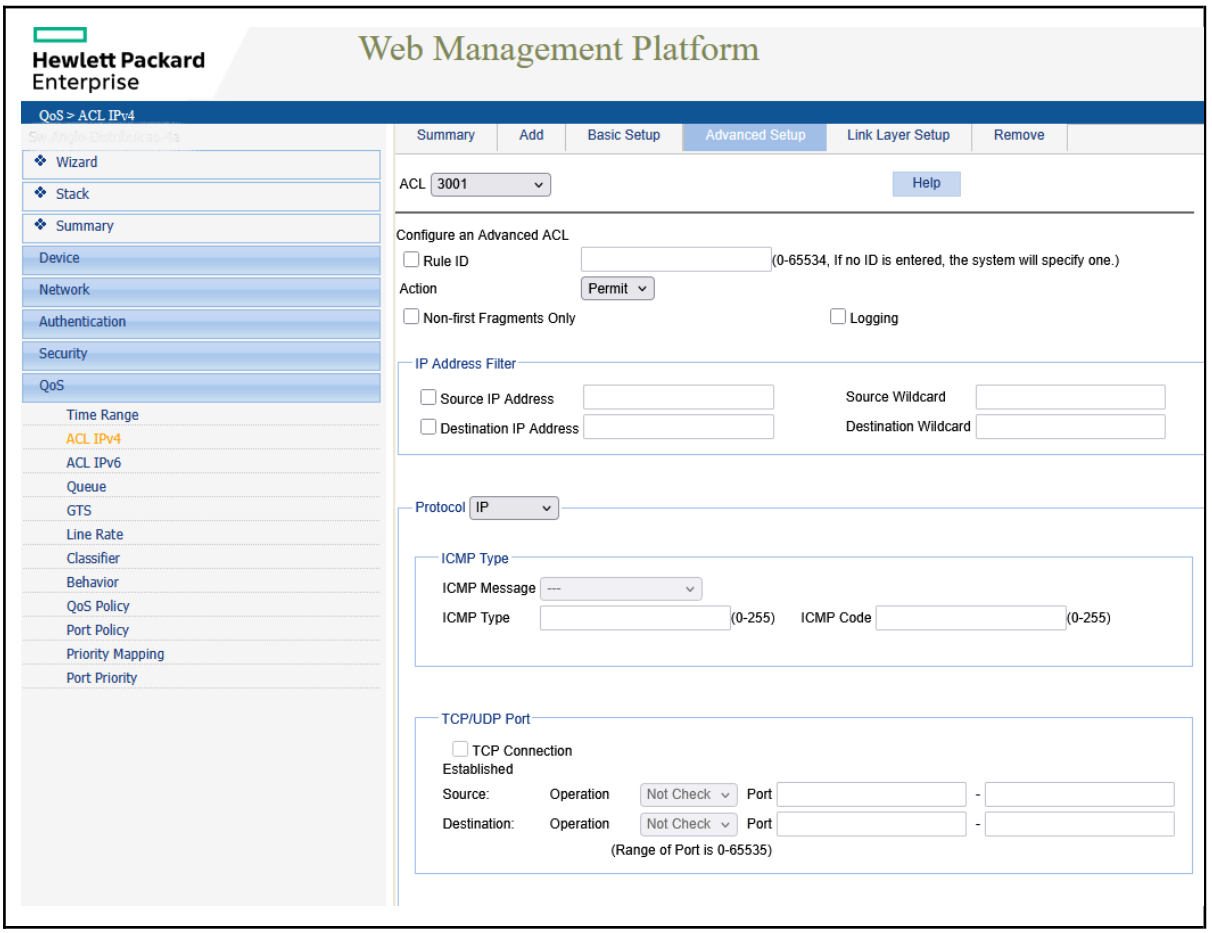
<switch> system-view
[switch] acl number 3000
[Huawei-acl-adv-3000] description Acesso_Web
[Huawei-acl-adv-3000] rule 5 permit tcp source 192.168.1.10 0.0.0.0 destination 192.168.1.100 0.0.0.0 destination-port eq 80
[Huawei-acl-adv-3000] rule 10 deny tcp destination 192.168.1.100 0.0.0.0 destination-port eq 80
rule 15 permit ip
[Huawei-acl-adv-3000] quit
[switch] interface Vlanif1
[Huawei-Vlanif10] traffic-filter outbound acl 3000

Edgecore ECS2100-28T (Web)



HP 1920-48 (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



5.8 Limitação de Acesso em Portas (*Port Security*)

A funcionalidade de limitação de acesso em portas, também conhecida como *Port Security*, é um recurso que permite restringir o número de endereços MAC permitidos em uma porta específica do switch. Ao limitar os endereços MAC autorizados em uma porta, o *Port Security* ajuda a prevenir o acesso não autorizado à rede através dessas portas e mitigar ataques como spoofing de MAC e a conexão de dispositivos não gerenciados.

O *Port Security* opera aprendendo os endereços MAC dos dispositivos conectados a uma porta do switch e armazenando esses endereços em uma tabela de endereços seguros (*secure MAC address table*) para essa porta específica. Uma vez que o número máximo de endereços MAC seguros permitido para uma porta é configurado, qualquer tentativa de conexão de um dispositivo com um endereço MAC não presente na tabela segura (após o limite ser atingido) acionará uma ação de segurança predefinida.

O *Port Security* oferece diferentes modos para aprender e configurar os endereços MAC seguros em uma porta:

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Aprendizagem Estática (*Static Learning*):** Os endereços MAC permitidos para uma porta são configurados manualmente pelo administrador através da interface de gerenciamento. Esses endereços são armazenados na configuração em execução e na configuração de inicialização. Este modo oferece o maior nível de controle de segurança.

- **Aprendizagem Dinâmica (*Dynamic Learning*):** O switch aprende automaticamente os endereços MAC dos dispositivos que se conectam à porta e os adiciona à tabela de endereços seguros. Esses endereços são armazenados apenas na configuração em execução e são perdidos após uma reinicialização do switch. Este modo oferece conveniência, mas pode ser menos seguro, pois qualquer dispositivo que se conectar primeiro pode ser autorizado.

- **Aprendizagem Fixa (*Sticky Learning*):** Uma combinação dos modos dinâmico e estático. O switch aprende dinamicamente os endereços MAC dos dispositivos conectados e os adiciona à tabela de endereços seguros. Além disso, esses endereços aprendidos dinamicamente podem ser salvos na configuração em execução, tornando-os persistentes após uma reinicialização. Este modo oferece um bom equilíbrio entre conveniência e segurança.

Quando uma violação de segurança ocorre (ou seja, um dispositivo com um endereço MAC não seguro tenta acessar a porta após o limite ser atingido), o switch pode realizar uma das seguintes ações configuradas:

- ***Protect*:** O switch descarta o tráfego com o endereço MAC de origem desconhecida, mas não envia nenhuma notificação de violação e não incrementa o contador de violações. Os dispositivos com endereços MAC seguros previamente aprendidos continuam a funcionar normalmente.

- ***Restrict*:** O switch descarta o tráfego com o endereço MAC de origem desconhecido e envia uma notificação de violação (por exemplo, via SNMP trap ou mensagem de log do sistema). Ele também incrementa o contador de violações. Os dispositivos com endereços MAC seguros previamente aprendidos continuam a funcionar normalmente.

- ***Shutdown*:** O switch desativa imediatamente a porta em estado de erro (*error-disabled*). A porta permanece desativada até que seja reativada manualmente pelo administrador através da interface de gerenciamento. Esta é a ação mais segura, pois impede completamente o acesso não autorizado através da porta. Uma notificação de violação também é geralmente enviada e o contador de violações é

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

incrementado.

Ao ativar a funcionalidade de *Port Security* nas portas do switch haverá uma melhor administração dos dispositivos conectados na rede. As vantagens do uso da limitação de acesso em Portas:

- **Prevenção de Acesso Não Autorizado:** Impede que dispositivos não autorizados se conectem à rede através de portas desocupadas ou comprometidas.
- **Mitigação de Ataques de *Spoofing* de MAC:** Dificulta que atacantes se façam passar por dispositivos legítimos alterando seus endereços MAC.
- **Controle de Dispositivos Conectados:** Permite um controle preciso sobre quais dispositivos podem acessar a rede através de portas específicas.
- **Aumento da Segurança da Rede:** Adiciona uma camada extra de segurança à infraestrutura de rede, complementando outras medidas de segurança.

Algumas considerações importantes sobre a configuração de *Port Security* em switches:

- **Número Máximo de Endereços MAC:** É importante definir um número máximo adequado de endereços MAC seguros permitidos por porta. Um valor muito baixo pode impedir a conexão de dispositivos legítimos (por exemplo, um computador conectado a um telefone VoIP, enquanto um valor muito alto pode reduzir a eficácia da segurança.
- **Modo de Aprendizagem:** A escolha do modo de aprendizagem depende dos requisitos de segurança e da facilidade de gerenciamento. O modo estático oferece maior segurança, mas requer mais administração manual. O modo *sticky* oferece a facilidade de aprendizado dinâmico e a possibilidade de guardar os endereços MAC na configuração de forma permanente.
- **Ação de Violação:** A ação de violação deve ser escolhida com base no nível de segurança desejado e no impacto potencial na disponibilidade da rede. O modo de desligamento é o mais seguro, mas pode interromper a conectividade de usuários legítimos se a configuração não for precisa.
- **Gerenciamento:** É importante monitorar as tabelas de endereços seguros e os eventos de violação para garantir a eficácia do *Port Security* e identificar possíveis problemas de segurança.

Na Tabela 40 estão exemplos da configuração em switches diversos.

Tabela 40. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)
switch> enable

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

switch# configure terminal
switch(config)# interface FastEthernet0/1
switch(config-if)# switchport mode access
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security maximum 1
switch(config-if)# switchport port-security violation shutdown
switch(config-if)# switchport port-security mac-address sticky

** Limita em um endereço MAC na porta F0/1 e aprende o primeiro endereço MAC que for detectado na porta. Em caso de violação, por exemplo a detecção de múltiplos endereços, a porta ficará em estado de err-disabled (inativada por motivo de violação).*

Para verificar o estado das proteções de portas

switch# show port-security interface FastEthernet0/1
switch# show port-security address

Huawei S5720-52X-LI (CLi)

<switch> system-view
[switch] interface GigabitEthernet 0/0/1
[switch-GigabitEthernet0/0/1] port link-type access
[switch-GigabitEthernet0/0/1] mac-limit maximum 1 action discard

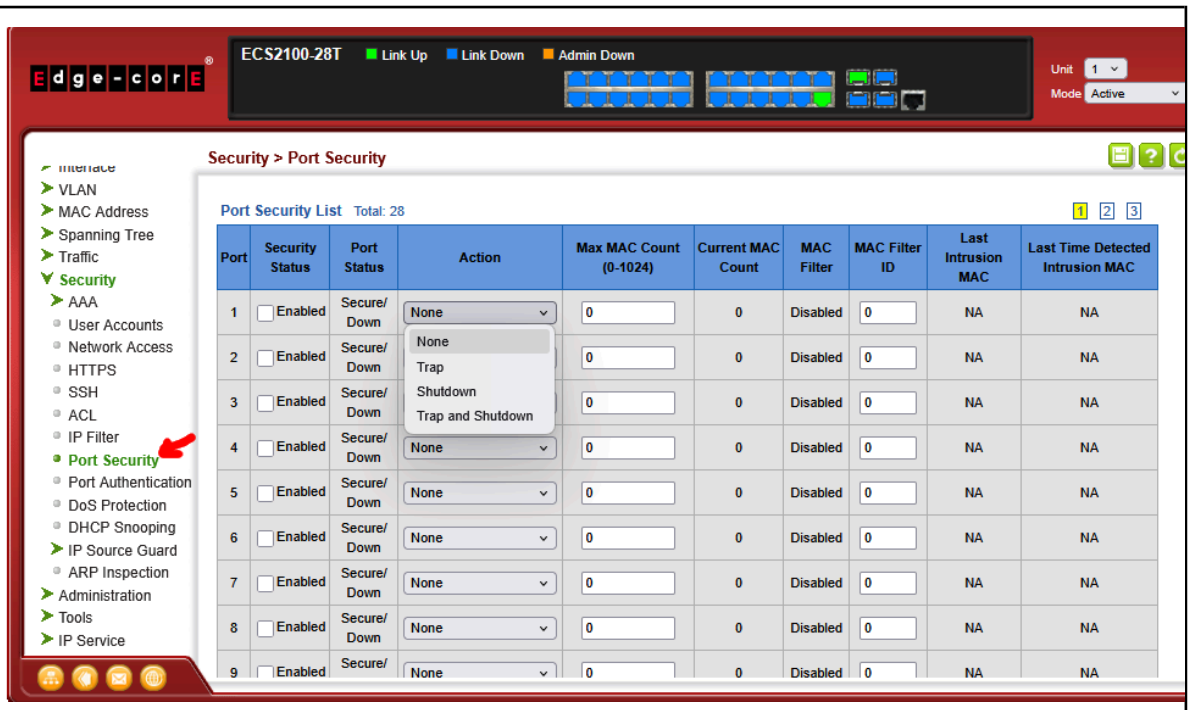
** Limita em um endereço MAC na porta F0/1 e aprende o primeiro endereço MAC que for detectado na porta. Em caso de violação, por exemplo a detecção de múltiplos endereços, a porta ficará em estado de err-disabled (inativada por motivo de violação).*

Para verificar o estado das proteções de portas

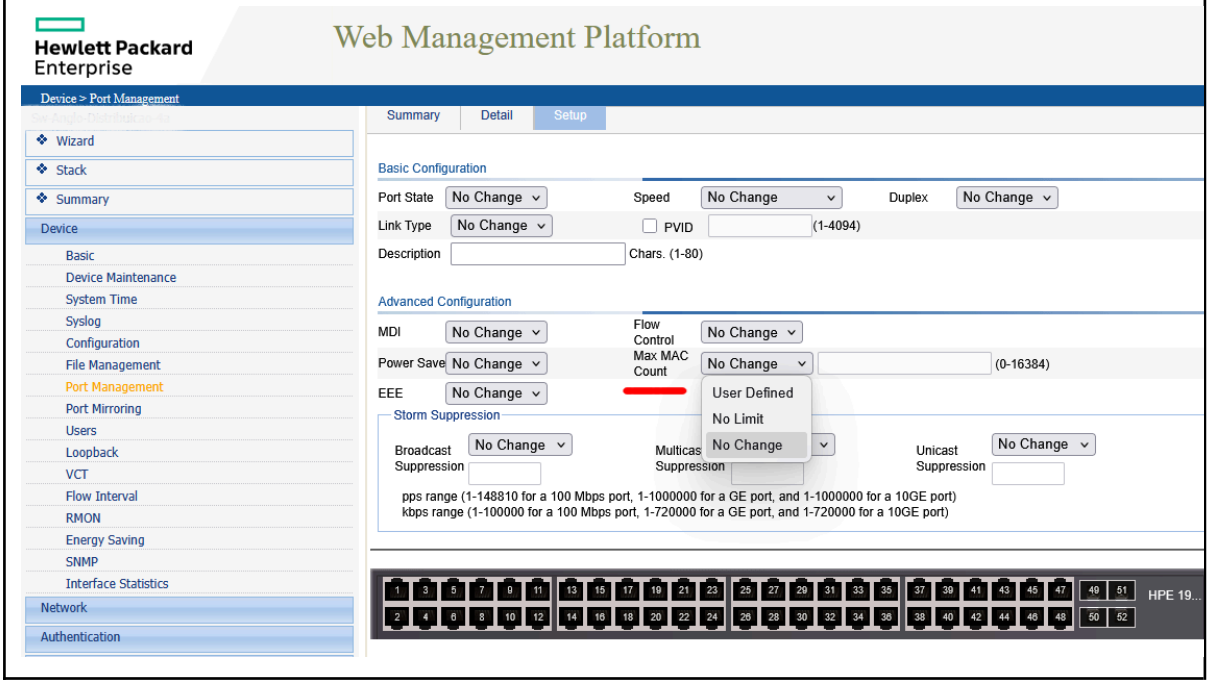
<switch> display mac-limit interface GigabitEthernet 0/0/1
<switch> display mac-address interface GigabitEthernet 0/0/1

Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



HP 1920-48 (Web)



5.9 QoS (Quality of Service)

A Qualidade de Serviço (*Quality of Service*), reconhecida pelo acrônimo QoS, em switches de camada 2 refere-se aos mecanismos implementados para priorizar diferentes tipos de tráfego de rede, garantindo um tratamento diferenciado para dados sensíveis a

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

atraso, *jitter* (variação no atraso) e perda de pacotes, como voz e vídeo em tempo real. Embora switches de camada 2 operem principalmente com base em endereços MAC e VLANs, eles podem utilizar alguns mecanismos de QoS para influenciar a forma como o tráfego é encaminhado dentro da mesma rede local (VLAN).

Redes para Iniciantes - QoS - https://www.youtube.com/watch?v=cvAsWF1GhtQ

A principal limitação dos switches de camada 2 para implementação de QoS avançado reside no fato de que eles não analisam as informações das camadas superiores (camadas 3 e 4), como endereços IP ou portas TCP/UDP, que são comumente usadas para classificar e priorizar o tráfego em roteadores de camada 3. No entanto, os switches de camada 2 podem utilizar informações presentes no cabeçalho Ethernet (IEEE 802.1Q) para implementar algumas formas de QoS.

Os mecanismos de QoS comuns em switches de camada 2 são:

- **IEEE 802.1p (*Priority Tagging*):** Este padrão define um campo de 3 bits no cabeçalho da *tag* 802.1Q (utilizada para identificação de VLANs) chamado ***Priority Code Point* (PCP)**. Esses 3 bits permitem atribuir um valor de prioridade (de 0 a 7, sendo 7 a maior prioridade) a cada quadro Ethernet.
    - Os switches de camada 2 que suportam 802.1p podem inspecionar esse campo PCP e utilizar o valor para priorizar o tráfego. Por exemplo, quadros com um valor PCP mais alto podem ser colocados em filas de saída com maior prioridade.
- **Filas de Saída (*Output Queues*):** Os switches utilizam múltiplas filas de saída por porta para armazenar temporariamente os quadros antes de serem transmitidos. A QoS em camadas 2 pode envolver a configuração de diferentes prioridades para essas filas.
    - **Filas de Alta Prioridade:** Quadros com marcações de alta prioridade (via 802.1p) são colocados nessas filas e são servidos primeiro, reduzindo a latência para tráfego sensível ao tempo.
    - **Filas de Baixa Prioridade:** Quadros com marcações de baixa prioridade são colocados nessas filas e podem sofrer mais atraso se houver congestionamento na porta.
- **Algoritmos de Agendamento de Filas:** Os switches utilizam algoritmos para determinar a ordem em que os quadros nas diferentes filas de saída são transmitidos. Alguns algoritmos comuns incluem:

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

    - ***Priority Queuing* (PQ):** Os quadros nas filas de maior prioridade são sempre transmitidos antes dos quadros nas filas de menor prioridade. Isso pode levar à fome (*starvation*) de tráfego de baixa prioridade se houver um fluxo constante de tráfego de alta prioridade.
    - ***Weighted Round Robin* (WRR):** Cada fila recebe uma certa quantidade de "peso" ou "tempo de serviço". As filas são atendidas em um ciclo, mas as filas com maior peso recebem mais tempo de transmissão. Isso evita a fome e garante alguma largura de banda para o tráfego de baixa prioridade.
    - ***Strict Priority* (SP):** Similar ao PQ, mas com uma prioridade estrita. O tráfego de menor prioridade só é transmitido quando todas as filas de maior prioridade estão vazias.
- **Marcação (*Remarking*) de Prioridade (CoS - *Class of Service*):** Alguns switches de camada 2 mais avançados podem ter a capacidade de marcar (ou remarcar) o campo PCP (CoS - *Class of Service*) dos quadros com base em certas regras.

É fundamental entender as limitações da QoS em switches de nível 2:

- **Falta de consciência da camada 3 e 4:** A incapacidade de inspecionar endereços IP e portas TCP/UDP limita severamente a granularidade da classificação do tráfego. A priorização é geralmente baseada em informações de camada 2, que podem não refletir a importância da aplicação ou do tipo de tráfego.
- **Escopo Local (Dentro da VLAN):** A priorização baseada em 802.1p é significativa dentro de uma única rede local (VLAN) onde os tags 802.1Q são mantidos. Ao rotear o tráfego para outras redes (camada 3), as informações de prioridade 802.1p podem não ser preservadas ou interpretadas da mesma forma pelos roteadores.
- **Confiabilidade da Marcação:** A marcação 802.1p depende da configuração correta dos dispositivos finais ou dos switches de borda que inserem ou modificam as tags 802.1Q. Se os dispositivos finais não marcarem o tráfego corretamente, a QoS em nível 2 pode não ser eficaz.

A QoS em switches de nível 2 é mais comumente utilizada para:

- **Priorização de Tráfego de Voz (VoIP) dentro da LAN:** Garantir que os pacotes de voz recebam prioridade sobre o tráfego de dados para minimizar a latência e o *jitter.* Isso geralmente envolve configurar os telefones IP para marcar o tráfego de voz com um valor PCP alto.
- **Priorização de Tráfego de Vídeo:** Similar ao VoIP, garantir uma melhor experiência para aplicações de videoconferência ou *streaming* de vídeo dentro da rede local.
- **Diferenciação de Tráfego Genérico:** Em cenários simples, pode-se priorizar o tráfego originário de certas portas consideradas mais importantes.
- **Limitação de banda em portas:** Limitar as taxas de *download* e *upload* com o uso de valores em bit/s.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Na Tabela 41 estão exemplos da configuração em switches diversos.

Tabela 41. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)

switch>enable
switch# configure terminal
switch(config)# interface FastEthernet0/9
switch(config-if)# srr-queue bandwidth limit 50

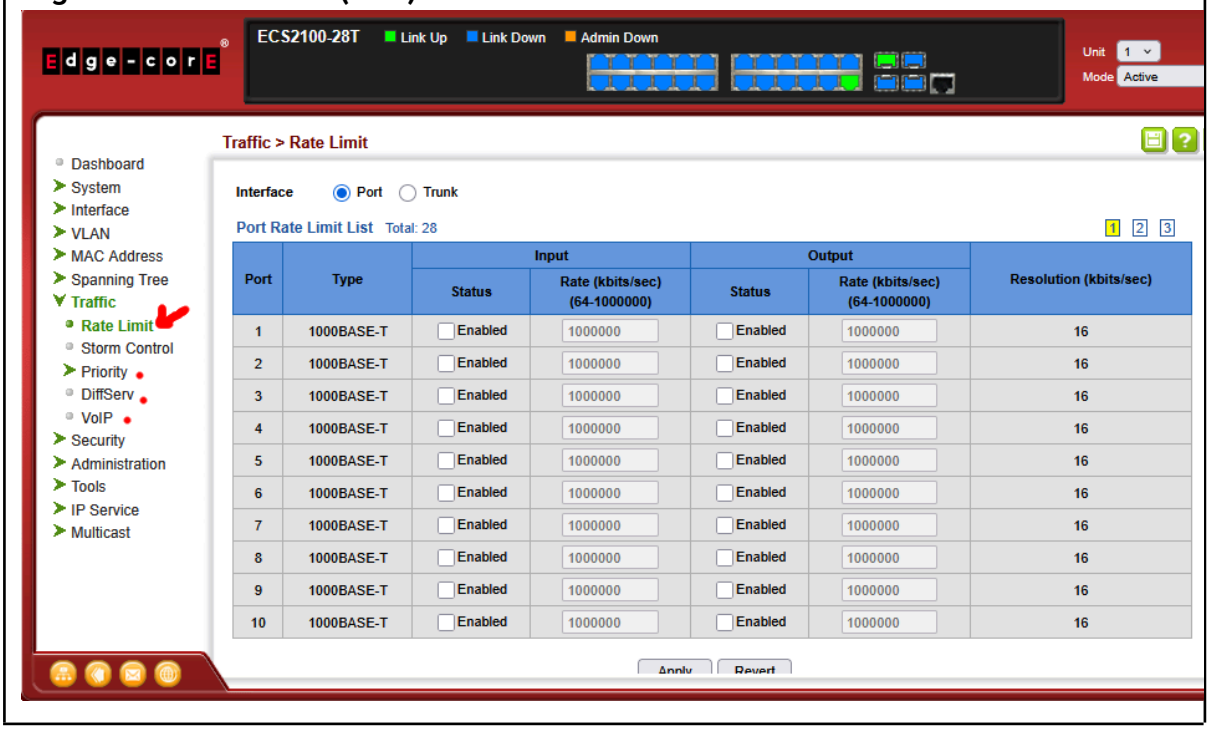
** Limita em 50% a velocidade da interface f0/9. Se a interface estiver configurada em 100 Mbit/s, ao aplicar limitação a largura de banda disponível será de 50 Mbit/s*

Huawei S5720-52X-LI (CLi)

<switch> system-view
[switch] interface GigabitEthernet 0/0/1
[switch-GigabitEthernet0/0/1] qos lr outbound cir 50000000 pir 50000000 green pass yellow pass red discard

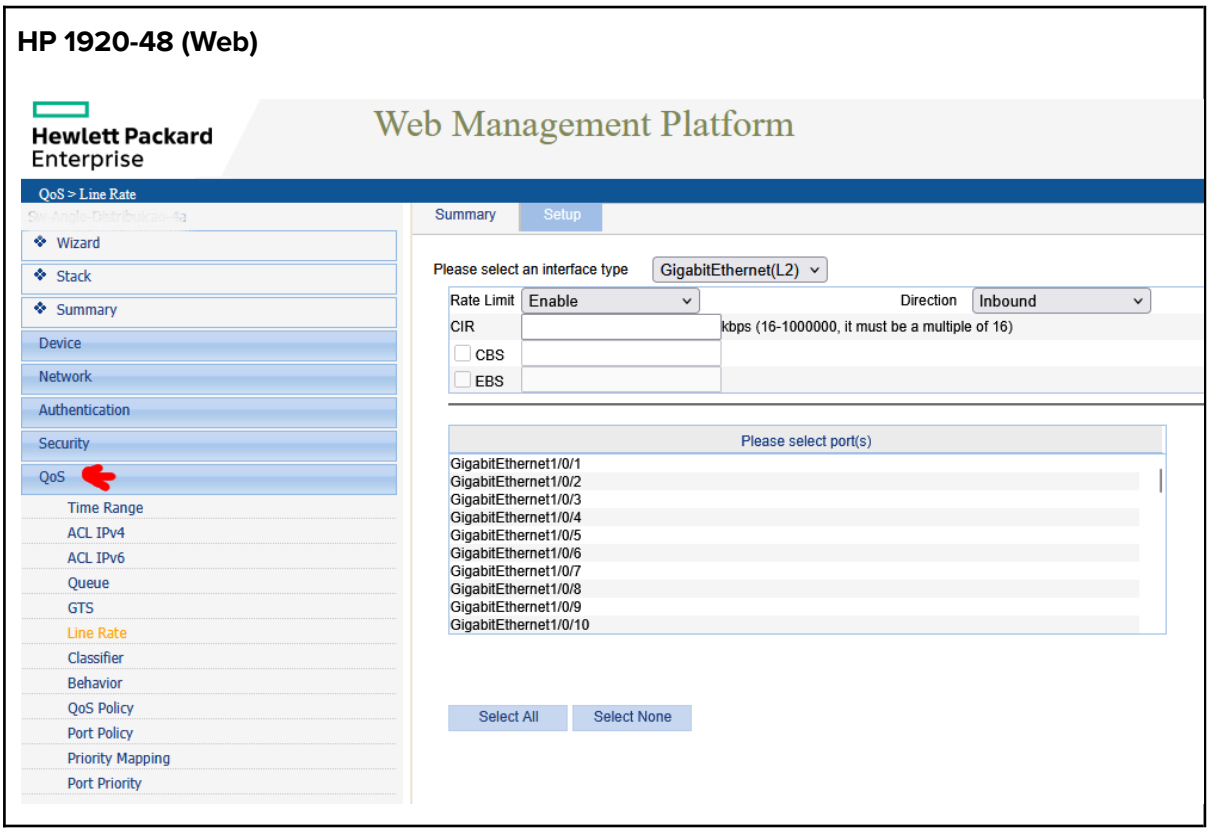
** Limita 50 Mbit/s a velocidade da interface g0/0/1.*

Edgecore ECS2100-28T (Web)



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

HP 1920-48 (Web)



5.10 Monitoramento de Recursos

O monitoramento dos recursos de um switch é uma rotina crítica para garantir o funcionamento, identificar gargalos de desempenho, diagnosticar problemas e planejar futuras expansões da rede. A maioria dos switches oferece uma variedade de comandos na sua interface de linha de comando (CLI) para visualizar o status e a utilização de seus recursos internos. Os recursos computacionais em switches de entrada são limitados e podem sofrer travamentos e indisponibilidade quando estiverem com alta carga.

Em casos onde há uma alta utilização da CPU pode indicar que o switch está sobrecarregado com tarefas de gerenciamento, processamento de tráfego excessivo ou até mesmo sendo alvo de ataques. A falta de memória pode levar à instabilidade do switch, falha no processamento de novas conexões ou até mesmo travamentos.

O volume de tráfego nas interfaces deve ser monitorado para identificar gargalos, problemas de conectividade, tais como erros, e padrões de uso da rede. Também é importante monitorar a tabela MAC que permite verificar os dispositivos conectados ao switch e identificar possíveis atividades suspeitas (por exemplo, um número excessivo de novos endereços MAC em uma porta).

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

O estado do *Spanning-Tree Protocol* (STP) com mudanças de estado de portas e de topologia podem indicar inconsistências na definição da ponte raiz ou desligamentos de switches que fazem parte da insistência do STP. Monitorar o estado do STP é importante para garantir que a rede esteja livre de *loops* e que a topologia esteja correta.

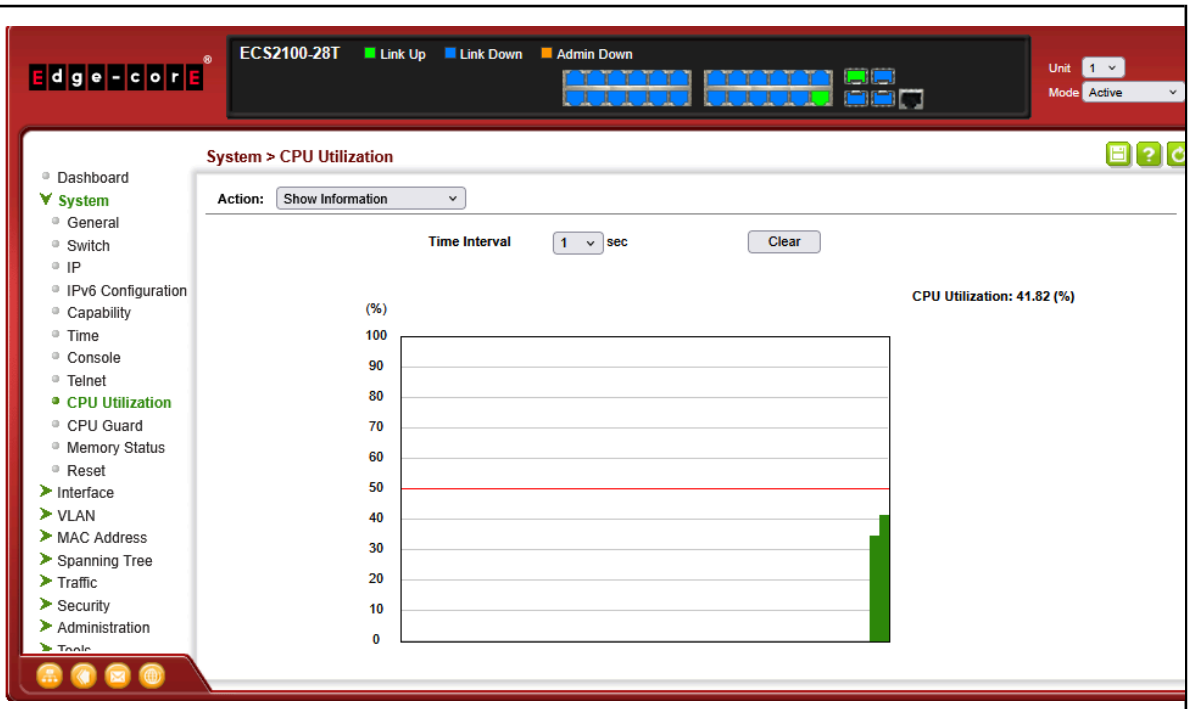
Embora não seja um monitoramento de recursos em si, os logs do sistema fornecem informações valiosas sobre eventos que ocorrem no switch, incluindo avisos de alta utilização de recursos, erros de interface e problemas de protocolo. Os logs que envolvem registros sobre o consumo de recursos do switch devem ser enviados para um servidor de logs remoto e analisados por meio de ferramentas que geram alertas em casos de anormalidades.

A interpretação dos dados de monitoramento é fundamental. Uma alta utilização da CPU ou memória pode indicar a necessidade de investigar a causa (por exemplo, tráfego anormal, configuração incorreta, ataque). Erros persistentes em uma interface podem indicar um problema físico com o cabo ou a porta. O monitoramento regular permite identificar tendências e planejar *upgrades* de capacidade antes que os problemas de desempenho impactem a rede. Na Tabela 42 estão exemplos da configuração em switches diversos.

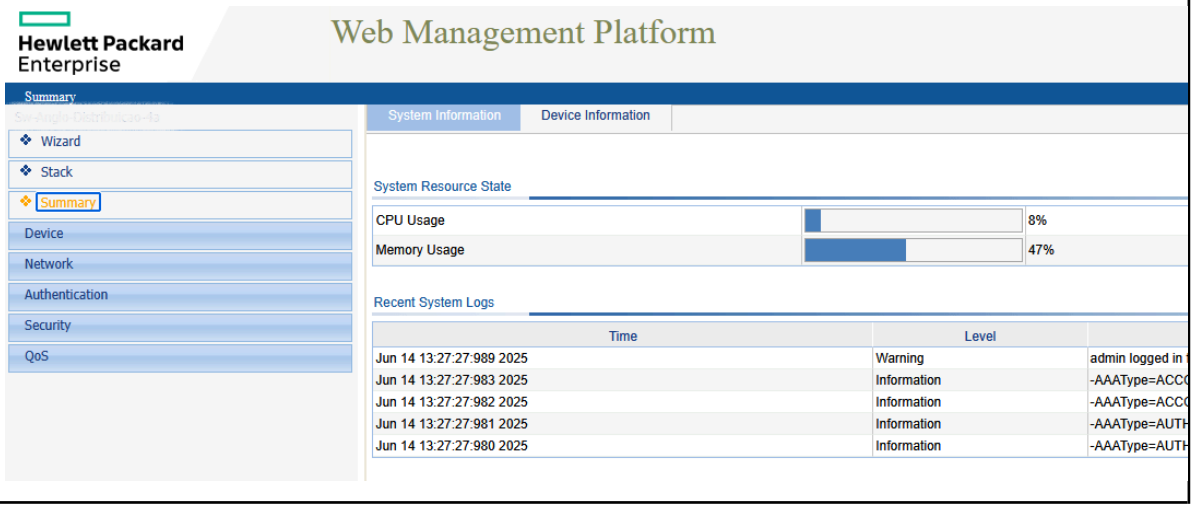
Tabela 42. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI) *switch>enable* *switch#show processes cpu* *switch#show memory* *switch# show memory summary* *switch# show processes*
Huawei S5720-52X-LI (CLi) *<switch> display cpu-usage* *<switch> display memory-usage* *<switch> display task*
Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



HP 1920-48 (Web)



5.11 Autenticação de Dispositivos

A autenticação de dispositivos, frequentemente implementada através do padrão IEEE 802.1X, é um protocolo de controle de acesso à rede baseado em porta para redes locais Ethernet (LANs) e redes sem fio (WLANs). Em switches gerenciáveis, o IEEE 802.1X fornece um mecanismo robusto para controlar o acesso de dispositivos à rede no nível da

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

porta, exigindo que um dispositivo (chamado suplicante) se autentique com um servidor de autenticação antes de ser permitido a trocar tráfego pela porta do switch.

Em ambientes de rede onde a segurança é uma preocupação, permitir que qualquer dispositivo se conecte livremente a uma porta do switch pode representar um risco significativo. Dispositivos não autorizados podem ser conectados para acessar recursos da rede, introduzir *malware* ou realizar ataques. A autenticação de dispositivos oferece uma solução para este problema, garantindo que apenas dispositivos confiáveis e autenticados tenham permissão para comunicar-se através da infraestrutura de rede.

O protocolo IEEE 802.1X envolve três componentes principais:

- **Suplicante (*Supplicant*):** O dispositivo final que deseja acessar a rede (por exemplo, um notebook, computador desktop, um telefone IP). O suplicante deve executar um software cliente 802.1X para se comunicar com o autenticador.

- **Autenticador (*Authenticator*):** O switch que controla o acesso à rede. O autenticador atua como um intermediário entre o suplicante e o servidor de autenticação. Ele recebe as credenciais do suplicante e as encaminha para o servidor de autenticação para verificação.

- **Servidor de Autenticação (*Authentication Server*):** Um servidor centralizado responsável por verificar as credenciais do suplicante e autorizar ou negar o acesso à rede. O protocolo RADIUS (*Remote Authentication Dial-In User Service*) é o servidor de autenticação mais comumente utilizado com o 802.1X. Outros protocolos como TACACS+ também podem ser usados em alguns cenários. Podem ser utilizadas as bases de usuários disponíveis no Microsoft AD (*Active Directory*) ou soluções em código-fonte aberto em Linux tal como FreeRadius que possibilita autenticação em outras fontes de dados.

  O processo de autenticação 802.1X geralmente segue os seguintes passos:

  1. **Detecção:** Quando um suplicante se conecta a uma porta do switch configurada para 802.1X, a porta é inicialmente colocada em um estado não autorizado. Apenas tráfego EAPOL (*Extensible Authentication Protocol over LAN*), o protocolo utilizado para a comunicação 802.1X, é permitido passar.

  2. **Solicitação de Identidade:** O autenticador envia uma solicitação de identidade (*EAP-Request/Identity*) ao suplicante.

  3. **Resposta de Identidade:** O suplicante responde com sua identidade (usuário e senha) em uma mensagem *EAP-Response/Identity*.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

4. **Autenticação:** O autenticador encaminha a identidade do suplicante e outras informações relevantes (como o endereço MAC da porta) para o servidor de autenticação utilizando o protocolo RADIUS.

5. **Processamento no Servidor de Autenticação:** O servidor RADIUS verifica as credenciais do suplicante em seu banco de dados (que pode ser local ou integrado a um sistema de diretório como o *Active Directory*). O servidor pode utilizar diferentes métodos de autenticação (por exemplo, senhas, certificados digitais).

6. **Autorização:** Se as credenciais forem válidas, o servidor RADIUS envia uma mensagem de sucesso (*RADIUS Access-Accept*) de volta ao autenticador, juntamente com informações de autorização, como a VLAN à qual o suplicante deve ser atribuído e quaisquer políticas de acesso específicas. Se as credenciais forem inválidas, o servidor envia uma mensagem de falha (*RADIUS Access-Reject*).

7. **Controle de Acesso:** Com base na resposta do servidor RADIUS, o autenticador (switch) autoriza ou nega o acesso do suplicante à rede na porta. Se o acesso for concedido, a porta é colocada em um estado autorizado, permitindo o tráfego normal de dados. Se o acesso for negado, a porta permanece em um estado não autorizado, bloqueando o tráfego do suplicante (exceto o tráfego EAPOL).

8. **Desconexão (Opcional):** O servidor RADIUS ou o suplicante podem iniciar uma sessão de desconexão, colocando a porta novamente em um estado não autorizado.

Com a utilização de autenticação de dispositivos e usuários em portas de switches são providos benefícios para a administração da rede, tais como:

- **Segurança Aprimorada:** Controla o acesso à rede no nível da porta, garantindo que apenas dispositivos autenticados possam se comunicar.
- **Prevenção de Acesso Não Autorizado:** Dificulta a conexão de dispositivos não gerenciados ou maliciosos à rede.
- **Controle Centralizado:** Permite o gerenciamento centralizado de políticas de acesso e autenticação através do servidor RADIUS.
- **Auditoria e Responsabilidade:** Facilita o rastreamento de qual usuário ou dispositivo estava conectado a qual porta e quando.
- **Suporte a Múltiplos Métodos de Autenticação:** O RADIUS suporta diversos métodos de autenticação, oferecendo flexibilidade na implementação de políticas de segurança.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Atribuição Dinâmica de VLANs:** Permite que os usuários sejam automaticamente colocados em VLANs específicas com base em suas credenciais ou função.

Existem diversos modos de operação 802.1X, os switches podem suportar diferentes modos, sendo o mais comum a autenticação baseada em porta (*Port-Based Authentication*). Uma breve descrição dos modos de operação do 802.1X são:

- ***Port-Based Authentication*:** A autenticação é aplicada a toda a porta física. Apenas um dispositivo pode ser autenticado por porta.
- ***MAC-Based Authentication* (MAB):** Utiliza o endereço MAC do dispositivo para autenticação, sem a necessidade de um software cliente 802.1X no dispositivo final. É útil para dispositivos que não suportam 802.1X (por exemplo, impressoras de rede, câmeras IP).
- ***Host Mode* (Single Host):** Apenas um suplicante é permitido por porta após a autenticação bem-sucedida.
- ***Multi-Host Mode*:** Permite que múltiplos hosts se conectem à mesma porta após a autenticação bem-sucedida do primeiro host.

Algumas considerações importantes sobre a implementação do 802.1X:

- **Infraestrutura RADIUS:** A implementação do 802.1X requer a configuração de um servidor RADIUS acessível pelos switches. É recomendado que o servidor esteja na mesma VLAN dos switches.
- **Configuração do Switch:** As portas do switch devem ser configuradas para habilitar a autenticação 802.1X e especificar o servidor RADIUS a ser utilizado. Devido a ser uma configuração por porta, um switch poderá ter portas com autenticação e outras sem autenticação.
- **Software Cliente:** Os dispositivos finais que precisam acessar a rede devem ter um software cliente 802.1X instalado e configurado. Em sistemas operacionais atuais o cliente é ativado por meio de um serviço que deverá estar ativo para solicitar a identificação para o usuário. No sistema operacional Microsoft Windows o nome do serviço em interfaces cabeadas é Configuração Automática com Fio (*Wired-AutoConfig*), que é mostrada na Figura 30.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

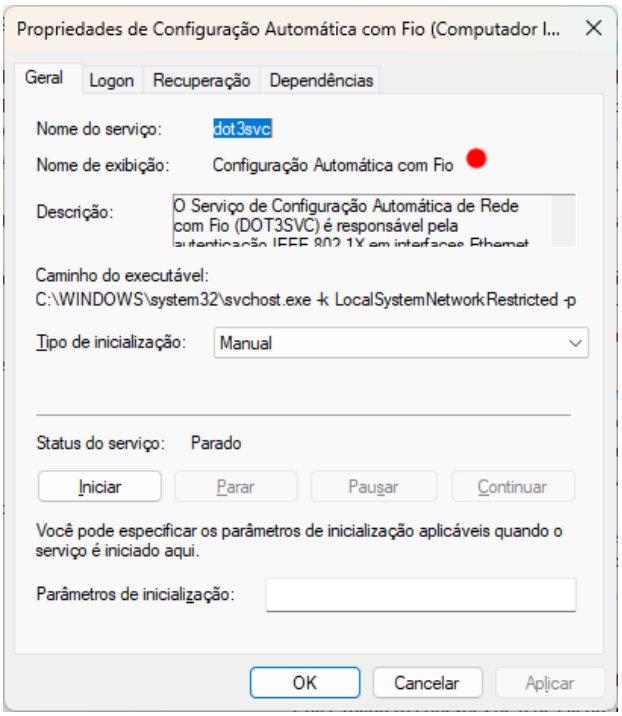


Figura 30. Serviço Configuração Automática com Fio para ativar a autenticação por 802.1X no Microsoft Windows.

- **Complexidade:** A implementação do 802.1X pode ser mais complexa do que simplesmente configurar autenticação em portas. Por exemplo, um usuário que não possua o serviço para solicitar a autenticação poderá relatar ao suporte de TI que a rede não está disponível. Outra questão é a necessidade de documentar com precisão as portas dos switches para liberar dispositivos que não tenham compatibilidade com o 802.1X, dispositivos tais como impressoras, câmeras IP ou com sistemas operacionais legados.
- **Testes:** É fundamental testar cuidadosamente a configuração do 802.1X para garantir que os dispositivos legítimos possam se autenticar corretamente e que o acesso não autorizado seja bloqueado.

Com o uso da funcionalidade do 802.1X, ao exigir a autenticação antes de conceder acesso, haverá melhorias na segurança da rede, ao impedir a conexão de dispositivos não autorizados e fornecer um mecanismo centralizado para gerenciamento de políticas de acesso. Na Tabela 43 estão exemplos da configuração em switches diversos.

Tabela 43. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)
switch> enable *switch# configure terminal*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

// Ativa a configuração para autenticação com IEEE 802.1x e os parâmetros do servidor RADIUS
switch(config)# aaa new-model
switch(config)# aaa authentication dot1x default group radius
switch(config)# radius-server host 192.168.10.10 auth-port 1812 acct-port 1813 key cisco123
switch(config)# dot1x system-auth-control

// Aplica na interface f0/1 a configuração IEEE 802.1x, limitando em apenas um MAC e com o período de 3600s para reautenticação
switch(config)# interface FastEthernet0/1
switch(config-if)# switchport mode access
switch(config-if)# authentication host-mode single-host
switch(config-if)# authentication port-control auto
switch(config-if)# dot1x pae authenticator
switch(config-if)# dot1x timeout quiet-period 5
switch(config-if)# dot1x timeout reauth-period 3600
switch(config-if)# spanning-tree portfast
switch(config-if)# end

Para mostrar o estado da configuração

switch# show dot1x
switch# show dot1x interface FastEthernet0/1
switch# show aaa servers

Huawei S5720-52X-LI (CLi)

<switch> system-view
// Define um template (modelo) para ser usado como configuração do servidor RADIUS
[switch] radius-server template RADIUS_TEMPLATE_1
// O parâmetro weight serve para definir a prioridade do servidor no template. Quanto maior o valor, maior a prioridade. Se houver outro servidor para ser secundário, o valor do weight deveria ser menor, por exemplo 70.
[switch-radius-server-RADIUS_TEMPLATE_1] radius-server authentication 192.168.10.10 1812 weight 80
[switch-radius-server-RADIUS_TEMPLATE_1] radius-server accounting 192.168.10.10 1813 weight 80
[switch-radius-server-RADIUS_TEMPLATE_1] radius-server shared-key simple Huawei123
[switch-radius-server-RADIUS_TEMPLATE_1] quit

// Ativa a configuração para autenticação com IEEE 802.1x
[switch] aaa
[switch-aaa] authentication-scheme dot1x_auth
[switch-aaa-authen-dot1x_auth] authentication-mode radius

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

[switch-aaa-authen-dot1x_auth] quit
[switch-aaa] quit

// Aplica as configurações do template para o servidor RADIUS.
[switch] domain default_admin
[switch-customize-domain-default_admin] authentication-scheme dot1x_auth
[switch-customize-domain-default_admin] radius-server RADIUS_TEMPLATE_1
[switch-customize-domain-default_admin] access-mode common
[switch-customize-domain-default_admin] quit

// Ativa globalmente a autenticação por IEEE 802.1x
[switch] dot1x enable

// Aplica na interface g0/0/1 a autenticação, limitando em 1 endereço MAC e com período para reautenticação de 3600s

[switch] interface GigabitEthernet 0/0/1
[switch-GigabitEthernet0/0/1] port link-type access
[switch-GigabitEthernet0/0/1] dot1x enable
[switch-GigabitEthernet0/0/1] dot1x authentication-method eap
[switch-GigabitEthernet0/0/1] dot1x port-method mac-based
[switch-GigabitEthernet0/0/1] dot1x max-user 1
[switch-GigabitEthernet0/0/1] dot1x reauthenticate enable
[switch-GigabitEthernet0/0/1] dot1x timer reauthenticate-period 3600
[switch-GigabitEthernet0/0/1] quit

Para mostrar o estado da configuração
<switch> display dot1x
<switch> display dot1x interface GigabitEthernet 0/0/1
<switch> display radius-server configuration
<switch> display aaa configuration

Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

HP 1920-48 (Web)

5.12 Layer 3

Tradicionalmente, a função primária de um switch era operar na camada 2 (Enlace de Dados) do modelo OSI, encaminhando tráfego com base em endereços MAC. No entanto, os switches de camada 3 (também conhecidos como switches *layer 3* ou *multilayer switches*) evoluíram para incorporar funcionalidades da camada 3 (Rede), permitindo realizar tarefas de roteamento, anteriormente exclusivas de roteadores dedicados. Essa capacidade de

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

combinar as funções de *switching* e roteamento em um único dispositivo oferece vantagens significativas em termos de desempenho, custo e complexidade da rede.

Redes para Iniciantes - Roteamento - https://www.youtube.com/watch?v=welZZeGxoxo

Estas são as principais funcionalidades de camada 3 em switches:

- **Roteamento IP:** A funcionalidade mais fundamental da camada 3 em switches é a capacidade de rotear tráfego entre diferentes redes IP (sub-redes). Isso significa que o switch pode analisar os endereços IP de destino nos pacotes e encaminhá-los para a próxima interface apropriada com base em suas tabelas de roteamento.

- **Interfaces Virtuais de Camada 3 (SVIs - *Switched Virtual Interfaces*):** Uma SVI é uma interface lógica associada a uma VLAN. Ela fornece um ponto de terminação de camada 3 para a VLAN dentro do switch. Cada VLAN pode ter uma SVI configurada com um endereço IP, permitindo que o switch atue como um gateway padrão para os dispositivos naquela VLAN e realize o roteamento entre diferentes VLANs (*inter-VLAN routing*).

- **Roteamento Estático:** Assim como em roteadores tradicionais, os switches de camada 3 permitem a configuração manual de rotas estáticas. Essas rotas definem explicitamente o caminho para redes de destino específicas. O roteamento estático é útil para redes pequenas ou para rotas específicas que não mudam frequentemente.

- **Protocolos de Roteamento Dinâmico:** Switches de camada 3 mais avançados suportam protocolos de roteamento dinâmico, como RIP (*Routing Information Protocol)*, OSPF (*Open Shortest Path First*) e BGP (*Border Gateway Protocol*). Esses protocolos permitem que o switch aprenda automaticamente sobre as topologias de rede e troque informações de roteamento com outros roteadores, ajustando as rotas dinamicamente em resposta a mudanças na rede. O suporte a protocolos de roteamento dinâmico torna os switches de camada 3 adequados para redes maiores e mais complexas.

- **Suporte a VLANs (*Virtual Local Area Networks*):** Embora as VLANs sejam uma funcionalidade primariamente de camada 2, sua integração com as capacidades de camada 3 é essencial. As SVIs fornecem a interface de camada 3 para cada VLAN, permitindo o roteamento entre elas. Os switches de camada 3 gerenciam o tráfego dentro de cada VLAN na camada 2 e o roteiam entre VLANs na camada 3. O desempenho do roteamento entre VLANs de forma interna no switch é muito superior

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

ao uso de portas tronco e interfaces virtuais que são limitadas pela velocidade da porta.

- **Listas de Controle de Acesso (ACLs) de camada 3 e 4:** Switches de camada 3 podem implementar ACLs que operam nas camadas 3 e 4, permitindo um controle de acesso mais granular baseado em endereços IP de origem e destino, protocolos (TCP, UDP, ICMP) e portas. Essas ACLs podem ser aplicadas às SVIs ou interfaces físicas para controlar o tráfego roteado.

- **QoS (*Quality of Service*) de camada 3 e 4:** Similarmente às ACLs, os switches de camada 3 podem implementar políticas de QoS baseadas em informações de camada 3 e 4, permitindo a priorização do tráfego com base em endereços IP, portas e outros parâmetros.

- **VRF (*Virtual Routing and Forwarding*):** Alguns switches de camada 3 suportam VRF, uma tecnologia que permite criar múltiplas instâncias de tabelas de roteamento dentro de um único switch. Isso possibilita a segmentação da rede em múltiplos domínios de roteamento lógico, oferecendo maior isolamento e segurança.

São cenários comuns para uso de switches de Camada 3:

- **Roteamento Inter-VLAN:** Permitir a comunicação eficiente entre diferentes VLANs dentro da mesma organização.
- **Camada de Acesso em Redes Corporativas:** Fornecer conectividade de camada 2 para os usuários finais e roteamento para a camada de agregação ou core.
- **Redes de Campus:** Conectar diferentes edifícios ou departamentos, fornecendo tanto switching local quanto roteamento entre eles.
- **Data Centers:** Utilizados para interconectar servidores e fornecer roteamento de alta velocidade entre diferentes segmentos de rede.

Em resumo, as funcionalidades de camada 3 em switches gerenciáveis representam uma evolução significativa na arquitetura de redes. Ao integrar capacidades de roteamento com as tradicionais funções de switching, esses dispositivos oferecem maior desempenho. Entretanto para uso de recursos mais avançados como ACLs complexas (firewall) e traduções de endereços usando NAT (*Network Address Translation*) poderá haver limitações nos recursos computacionais do switch com volumes maiores de tráfego e número de conexões. Na Tabela 44 estão exemplos da configuração em switches diversos.

Tabela 44. Exemplos da configuração em switches diversos.

Cisco 2960 (CLI)
switch>enable

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

switch#conf t
switch(config)# ip routing

// Ao ativar o roteamento, as interfaces virtuais configuradas no switch podem servir como gateway para os hosts na VLAN

Para visualizar a tabela de roteamento
switch#show ip route

Huawei S5720-52X-LI (CLi)

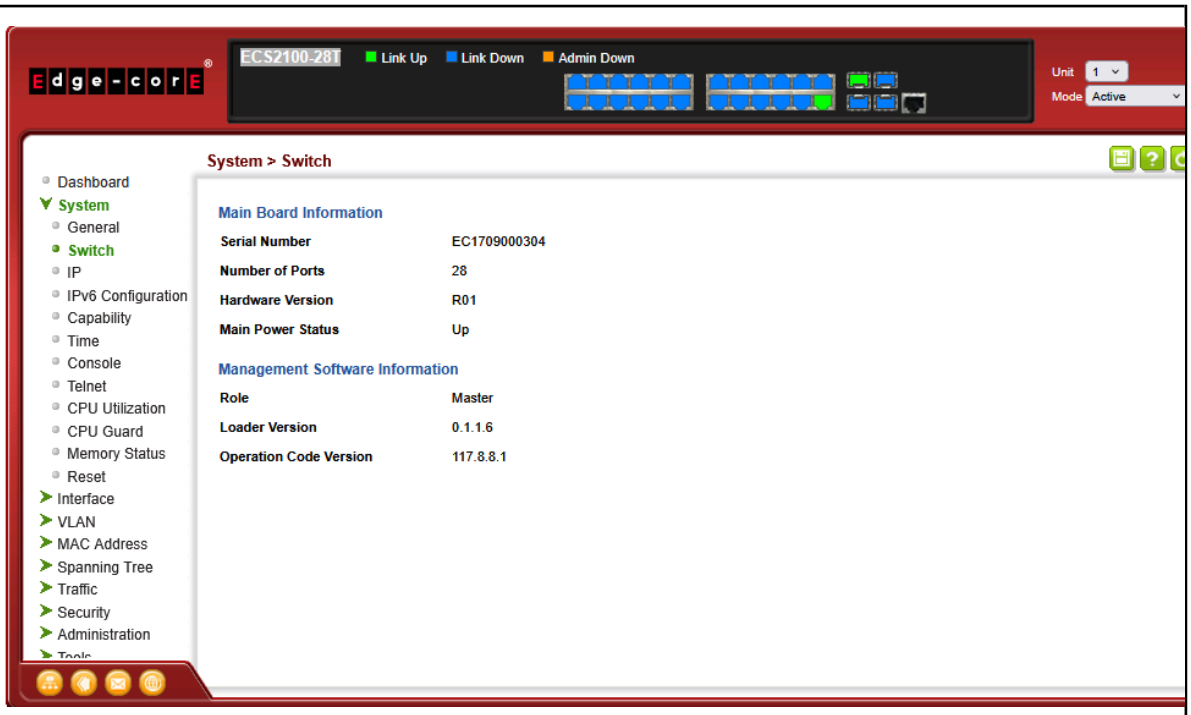
<switch> system-view
// Cria uma interface virtual na VLAN e configura um endereço IP
[switch] interface Vlanif10
[switch-Vlanif10] ip address 192.168.10.1 24
[switch-Vlanif10] quit

// Desativa as funcionalidades de switching na porta g0/0/24 e configura um endereço IP. Esta porta terá as funcionalidades de uma interface de rede tal como em um roteador.
[switch] interface GigabitEthernet 0/0/24
[switch-GigabitEthernet0/0/24] undo portswitch
[switch-GigabitEthernet0/0/24] ip address 10.0.0.1 30
[switch-GigabitEthernet0/0/24] quit

** Este switch não possui um comando de ativação global para roteamento, ao configurar uma interface com endereço IP ou utilizar o comando “undo portswitch” o roteamento ficará ativo.*

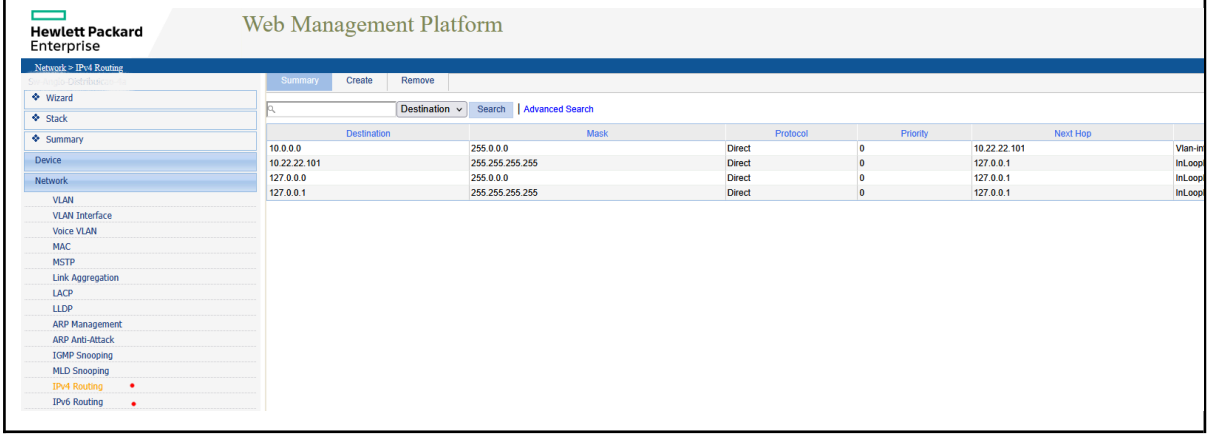
Edgecore ECS2100-28T (Web)

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional



A versão de firmware deste modelo não possui funcionalidades de roteamento

HP 1920-48 (Web)



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

6) Cenários de Aplicação

Após a exploração dos fundamentos da configuração e das funcionalidades avançadas dos switches gerenciáveis, este capítulo tem como objetivo consolidar esse conhecimento através da análise de cenários de aplicação prática. Compreender como implementar e configurar recursos específicos em situações reais é fundamental para o desenvolvimento de competências na administração de switches gerenciáveis.

Os cenários de aplicação utilizados como estudos de caso investigam a **Implementação de VLANs** para segmentação lógica e otimização do tráfego, passando pela **Ativação de dispositivos VoIP** com a garantia da qualidade de serviço necessária e a configuração de **Redundância de Links** para assegurar a alta disponibilidade da rede. Também são explorados a implementação de topologias específicas, como a **Topologia em Anel**, e as considerações para sua configuração em um ambiente gerenciado.

Cada cenário será detalhado, apresentando os desafios específicos, as funcionalidades dos switches gerenciáveis relevantes para a solução e as considerações práticas para uma implementação com sucesso. Ao analisar estes exemplos, será possível visualizar a aplicação prática dos conceitos e funcionalidades em switches gerenciáveis em uma rede local corporativa.

6.1 Implementação de VLANs

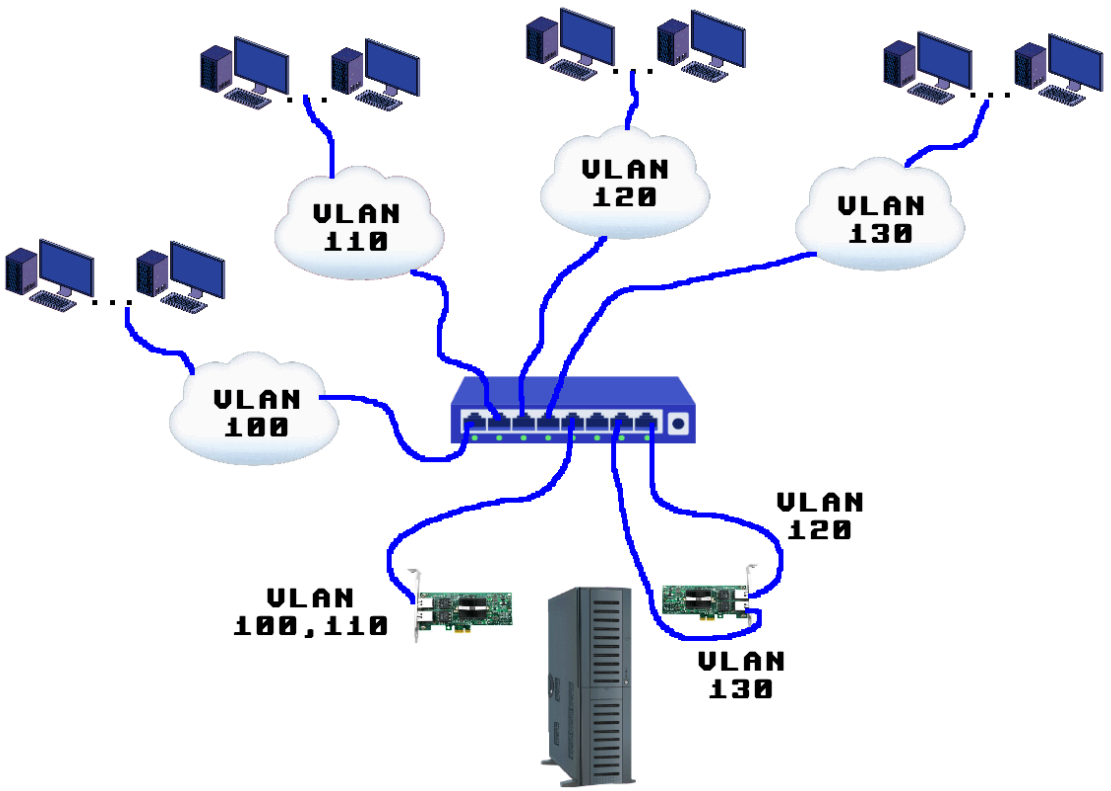
O uso de VLANs em redes corporativas tem como objetivo separar logicamente os segmentos de rede de acordo com a aplicação dos hosts. Por exemplo, o gerenciamento de dispositivos tais como switches deve ficar separado da rede onde usuários têm acesso. Este isolamento permite melhor controle e evita que um host não autorizado esteja na mesma rede lógica de um dispositivo ou serviço crítico na infraestrutura. Por exemplo, em uma rede sem fios corporativa WLAN (*Wireless Local Area Network*) o acesso de convidados deverá ficar em uma VLAN separada dos usuários administrativos . Esta configuração é realizada por meio da criação de um SSID (*Service Set Identifier*) atrelado a uma VLAN, por exemplo a rede “Convidados” na VLAN 120 e a rede “Empresa” na VLAN 200, onde o dispositivo cliente ao se associar na rede “Convidados” receberá endereçamento IP diferente da rede administrativa “Empresa”. O mesmo se aplica para serviços de impressão com uso de servidores para autorizar e contabilizar o uso de impressões. A VLAN das impressoras faz o isolamento dos dispositivos da rede dos dispositivos de usuários. Desta forma, as impressoras somente estarão disponíveis para impressão passando pelo servidor e não sendo descobertas pelo sistema operacional no hosts dos usuários. Outro caso é para para

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

dispositivos como telefones IP e câmeras que devem ter comunicação apenas com o servidor e não acesso direto a partir dos dispositivos de usuários.

No caso de servidores, a comunicação interna de serviços entre servidores distintos deve compartilhar de uma mesma VLAN. Por exemplo, entre um servidor de aplicações e um servidor de banco de dados, poderá haver uma VLAN isolada que permita a comunicação das conexões entre a aplicação e o banco de dados. Para melhorar o desempenho em servidores de arquivos pode-se utilizar múltiplas interfaces físicas em VLANs diferentes que participem das VLANs administrativas onde ficam os clientes. Desta forma, poderá ser evitada a necessidade de roteamento entre os hosts clientes e o acesso ao servidor de arquivos.

Na Figura 31, um exemplo de um servidor de arquivos com múltiplas interfaces de rede, com o uso de portas tronco e portas acesso em VLANs administrativas. As VLANs 100 e 110 estão associadas a uma mesma interface física, em uma porta tronco no switch. Haverá a limitação de largura de banda da interface do switch e do servidor para o tráfego das VLANs 100 e 110. Nos casos das VLANs 120 e 130 tem uma interface exclusiva para uma delas no servidor. Desta forma, haverá a disponibilização na íntegra da largura de banda da interface para cada VLAN ao acessar o servidor. Outra vantagem no cenário da Figura 31 é que o servidor terá acesso direto a cada uma das VLANs, sem a necessidade de realizar roteamento que poderá afetar negativamente o desempenho do serviço.



Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Figura 31. Exemplo de servidor de arquivos com múltiplas interfaces físicas

Na implementação deverá ser considerada a forma de agrupamento para definir as VLANs. A abrangência geográfica pode ser um critério de escolha, ao definir um prédio, andar, unidade organizacional ou atividade comum entre os hosts. Não há limite mínimo na quantidade de hosts para estarem associados a uma VLAN, entretanto não é recomendado utilizar um grande número de VLANs sem necessidade.

A relação entre os hosts que fazem parte da mesma VLAN tem a ver com a afinidade entre eles e a quantidade de hosts envolvidos. Um limite máximo aceitável de hosts por VLAN fica em torno de 200, mais que isto é uma boa prática dividir em mais de uma VLAN. Por exemplo, hosts que são de uso administrativo em um mesmo prédio poderiam ficar em uma mesma VLAN. Entretanto, se estes hosts fazem parte de setores com relações distintas, tais como hosts administrativos da direção e hosts administrativos que controlam o estoque, devem ficar em VLANs separadas. Esta avaliação de VLANs deverá ser realizada pela área técnica junto a gestão administrativa para definir o melhor cenário.

Outra definição importante está relacionada ao endereçamento IP a ser utilizado nas VLANs. O uso de identificação de VLAN com alguma associação ao prefixo de rede IP auxilia na administração e organização da rede. Por exemplo, ao definir uma VLAN ID **120**, uma alternativa para o prefixo de rede IPv4 seria 172.17.**120**.0/22, 192.168.**120**.0/24 ou 10.**120**.0.0/16. Assim, quando houver o recebimento de um IP, o suporte técnico poderá identificar imediatamente em qual VLAN está conectado um host ou um administrador de redes poderá alterar as regras de firewall ou identificar a origem de um fluxo de rede rapidamente.

A rotina de administração de VLANs nos switches é basicamente:

- **Criação de VLAN**: criar VLANs por meio da identificação e adicionar um nome textual para facilitar. Por exemplo, VLAN ID 100 e nome “Andar1”.
- **Associar VLAN nas portas de acesso**: associar a VLAN em portas de acesso ou de forma *untagged* na porta do switch. Nesta etapa o ponto de rede do dispositivo deve estar identificado ou realizar a identificação pelo endereço MAC da interface de rede.
- **Associar VLANs às portas tronco**: associar VLANs em portas tronco ou de forma tagged. Nesta etapa ao associar múltiplas VLANs em um porta do switch haverá a mudança de porta de acesso para porta tronco ou híbrida. As VLANs deverão ser as mesmas nas portas dos dois lados da conexão. Deverão ser configuradas apenas as VLANs que existam do outro lado da conexão.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Alterações de portas**: em caso de alteração de portas, por exemplo a troca de um ponto de rede em um dispositivo, deverá ser feita a alteração da VLAN para a nova porta. Se houver identificação do novo ponto de rede, será apenas a associação da VLAN correta na nova porta. Em caso de não haver esta informação, utilizar o endereço MAC do dispositivo, localizar na tabela MAC do switch e associar a VLAN correta na nova porta.
- **Adição de nova VLAN:** ao adicionar uma nova VLAN deverá ser criada em todos os switches onde há dispositivos ou uplinks que levem tráfego para onde há dispositivos nesta VLAN. Em ambientes onde existam um número grande de switches esta tarefa poderá ser bastante trabalhosa. Existem protocolos para propagação de VLANs, tais como VTP (*Virtual Trunking Protocol*) da Cisco, que é proprietário, ou o GVRP (*GARP VLAN Registration Protocol)*, que é aberto, entretanto dependem da compatibilidade de todos os switches instalados no parque.
- **Definição de interface de gateway**: para haver roteamento entre VLANs deverá ser criada uma interface em um roteador com endereço IP para responder como *gateway* para cada VLAN. Portanto, deverá haver uma interface no roteador na VLAN para poder encaminhar pacotes, esta interface pode ser física ou virtual (subinterface). É importante observar que não há obrigatoriedade de haver uma interface no roteador para rotear pacotes para cada VLAN criada, por exemplo uma VLAN que é usada para comunicação somente com dispositivos internos não precisaria acessar hosts em outras VLANs e não precisaria de um *gateway*. Por exemplo, uma câmera IP não precisaria acessar à Internet, somente o servidor de câmeras.

Na Figura 32, uma configuração de VLANs e portas associadas em um switch Intelbrás modelo SG 2404. Na configuração estão VLANs associadas a portas de acesso e portas tronco. Por exemplo, a VLAN 233 é usada para serviços de impressão. Esta VLAN está associada às portas 20, 23 e 24. A porta 20 tem uma impressora conectada e está configurada como acesso (*untag*). As portas 23 e 24 são portas de *uplink* e estão configuradas como portas tronco (*tagged*) para prover a comunicação com os demais dispositivos que participam da VLAN das impressoras.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

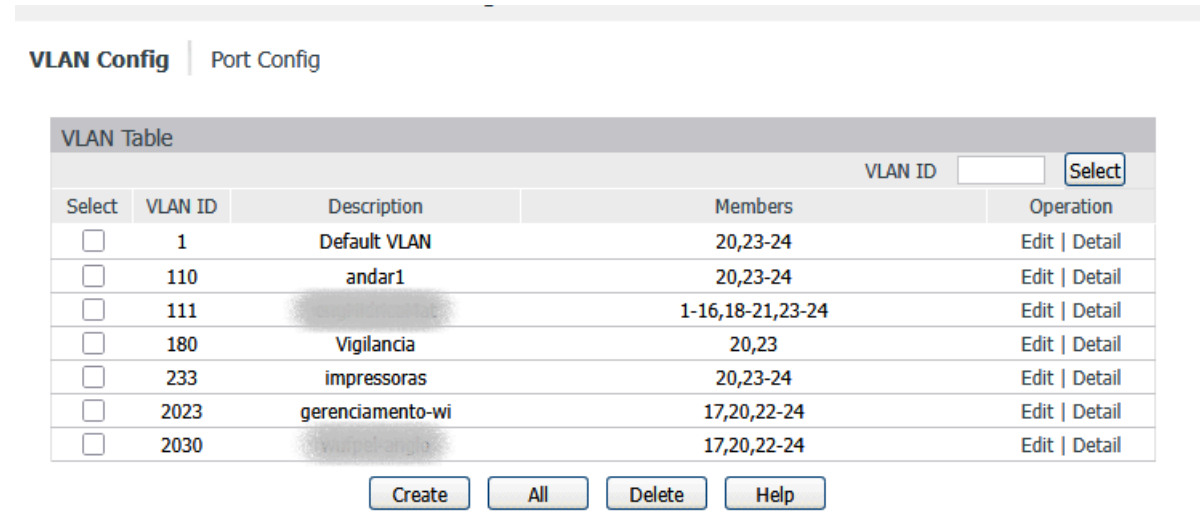


Figura 32. Configuração de VLANs e associação de portas.

Na Figura 33, um exemplo de configurações de VLANs em um roteador em sistema operacional Linux. A interface física do servidor Linux está conectada a uma porta do tipo tronco em um switch e para as VLANs associadas a porta são criadas interfaces virtuais e os endereços IP serão os gateways para encaminhamento dos pacotes.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

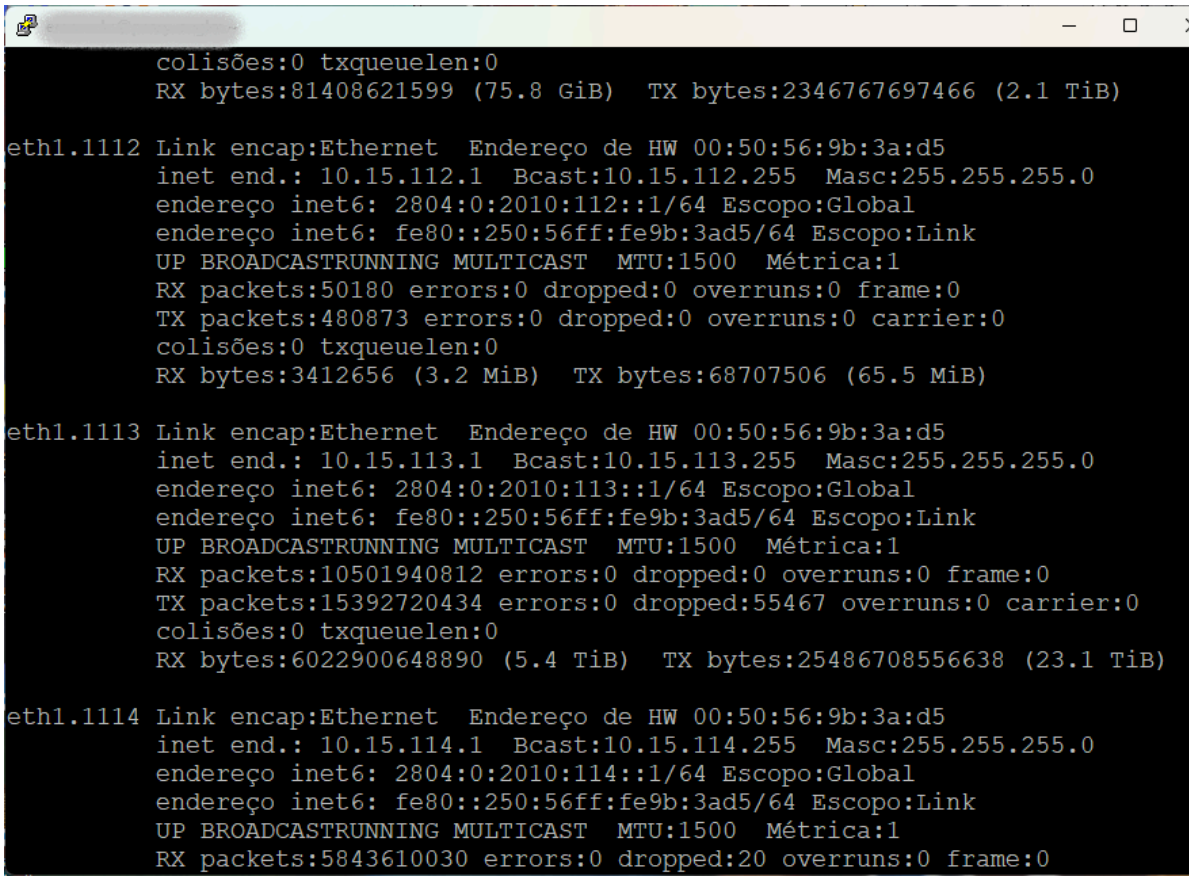


Figura 33. Configuração de interfaces virtuais em um roteador Linux.

Na Figura 34 está um diagrama representando uma rede local corporativa com diversos serviços, tais como câmeras de vigilância, impressoras, telefonia IP e rede sem fios, que devem usar VLANs para serem isolados do resto da rede. Além disso, a rede onde ficam os servidores e o gerenciamento dos dispositivos deve ficar em uma VLAN separada. Normalmente, a VLAN 1 é usada para o gerenciamento de dispositivos. Dependendo do número de hosts existentes na rede local ou na disposição da instalação, se em prédios distintos, em ambientes de trabalho setorizados ou em múltiplos andares de um único prédio, outras VLANs podem ser criadas para espelhar as particularidades do serviços disponibilizados para os agrupamentos de hosts.

O tráfego dos dispositivos será enviado para os servidores, por exemplo para o servidor de câmeras no caso da VLAN de câmeras de vigilância. Para evitar o roteamento desnecessário, o servidor de câmeras deverá possuir uma interface na VLAN das câmeras. Para acesso remoto a este servidor, deverá ser habilitada outra interface de rede em uma VLAN com endereços acessíveis remotamente e esta lógica de configuração se aplica aos outros serviços.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

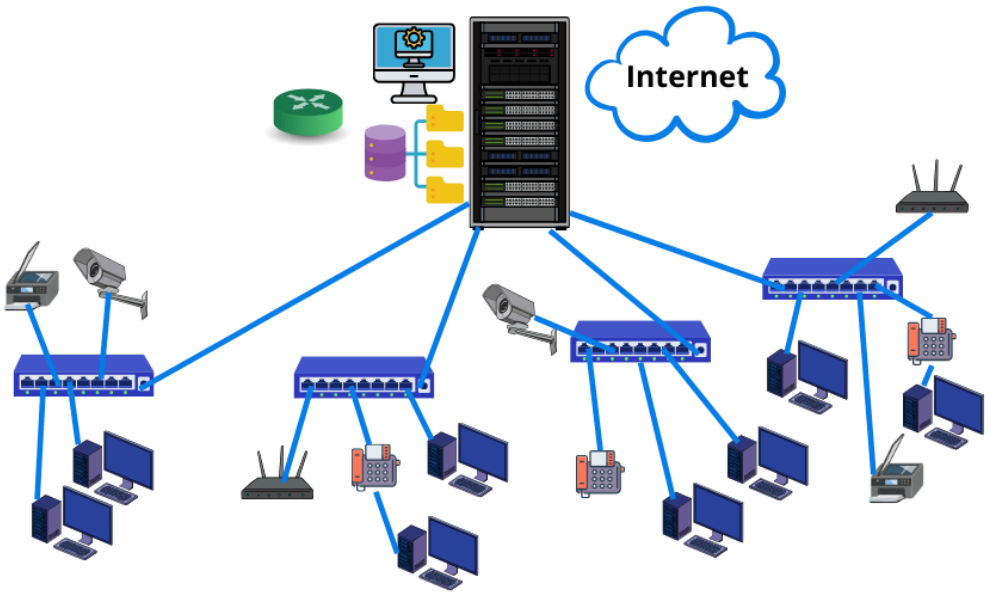


Figura 34. Ambiente corporativo com uso de VLANs.

Uma observação importante é evitar que as VLANs com grande volume de tráfego sejam repassadas por diversos *uplinks* entre os switches. Em caso de volumes grandes de tráfego ou até mesmo uma quantidade de pacotes em broadcast serão transmitidos pelas portas tronco entre os switches. Portanto, evitar a configuração de VLANs desnecessárias entre portas tronco e usar VLANs que necessitem passar por diversos switches.

6.2 Ativação de dispositivos VoIP

A configuração de dispositivos VoIP (Voz sobre IP) possui configurações específicas em switches. Nos casos onde o dispositivo estiver conectado sozinho em uma porta do switch bastaria associar a VLAN usada para o serviço de VoIP em modo acesso (*untagged*). Entretanto, é comum o uso de telefones IP na mesma porta onde já existem outros dispositivos, comumente um computador devido ao aproveitamento da infraestrutura existente. Nestes casos a porta do switch deverá ser configurada como um porta híbrida (*hybrid*), associando a VLAN de telefonia como *tagged* e a VLAN usada no computador como *untagged*. Nesta configuração o telefone IP funciona como um switch de duas portas permitindo que o computador tenha acesso à rede da VLAN original.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Introdução a VoIP (Voice over IP) - https://youtu.be/TO8CLknltwM

Na Figura 35, um exemplo de compartilhamento de porta entre um dispositivo de telefonia VoIP e um computador. Neste caso, a VLAN da telefonia não será repassada para a porta onde está ligado o computador, o qual não interpreta pacotes marcados com a *tag* de VLAN.

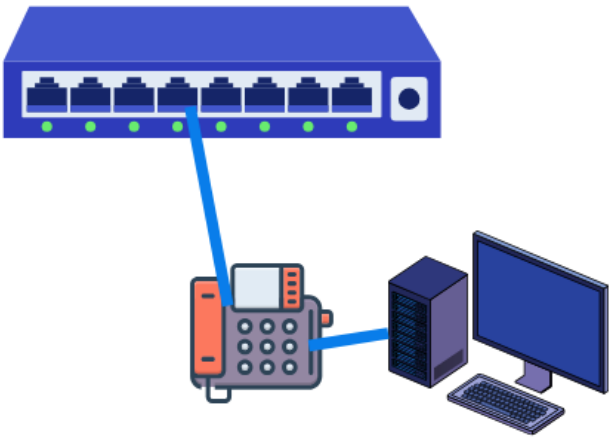


Figura 35. Conexão com VoiceVLAN em porta híbrida

Outra possibilidade é o uso da funcionalidade de *Voice VLAN*. Nesta configuração são criadas ACLs para associar a VLAN de telefonia de acordo com o prefixo o endereço MAC dos dispositivos. Desta forma, ao conectar um dispositivo que seja identificado com a regra de filtragem, será aplicada a VLAN de telefonia e, dependendo do switch, a marcação e a priorização do tráfego. Na Figura 36, um exemplo de configuração em um switch HP modelo 1920 para criar uma máscara com o prefixo dos endereços MAC dos dispositivos de telefonia IP. Os endereços MAC deverão seguir um padrão para essas regras serem eficientes.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

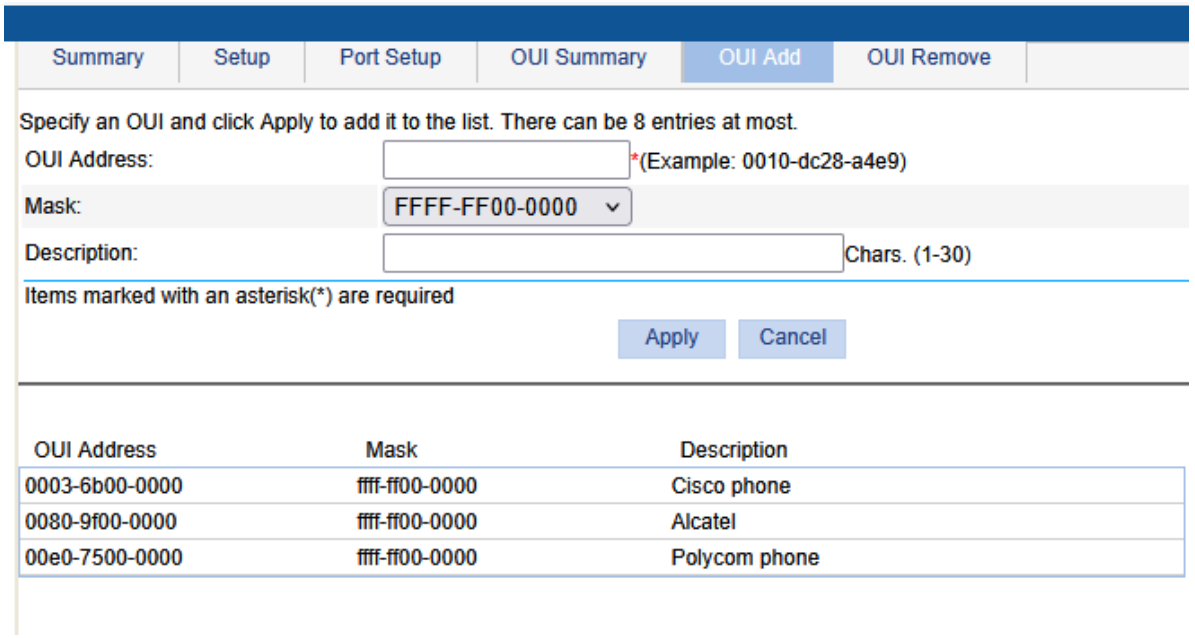


Figura 36. Exemplo de configuração de prefixo para identificação de dispositivo VoIP.

6.3 Cascatemento (Uplink)

O cascateamento entre switches é um procedimento comum e fundamental para expansão de portas para conexões de dispositivos em uma rede local. Os switches possuem um número de portas físicas limitado, comumente de 8, 16, 24, 48 ou 96 portas, e em switches modulares podendo chegar às centenas de portas. Em switches com capacidade de empilhamento (*stacking*) é possível o uso de conexões de alta velocidade em curtas distâncias, agrupando vários switches com alto desempenho de comutação e gerenciamento centralizado, tornando o empilhamento uma forma de criar um único switch virtual com vários switches físicos agrupados. Porém, as conexões para empilhamento utilizam cabos de curta distância, de 50cm a 1m em média, e proprietários de cada fabricante, com custos bastante elevados. Na Figura 37. um exemplo de conexões com cabos proprietários para empilhamento (*stacking*) em switches.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

Figura 37. Conexões para empilhamento de switches

Entretanto, em redes corporativas os switches não estão todos concentrados próximos aos dispositivos finais e haverá a necessidade de interconectar switches dispersos. Estas interconexões podem ser realizadas por par metálico, em distâncias menores que 100 metros, ou deverá ser usado fibra óptica em distâncias maiores. Em geral, é recomendável limitar o número de níveis de switches interconectados em cascata (por exemplo, não mais que 2 ou 3 níveis). Cada nível adicional pode introduzir latência e aumentar a complexidade da resolução de problemas, porém não há restrição no número de switches que podem ser cascateados.

Quantos switches podem ser cascateados? - https://youtu.be/9GUnjtlTv7Q

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Cascateamento de Switches: recorde com 30 switches cascateados - https://youtu.be/qV9iSyGbiwQ

É importante diferenciar e comparar o cascateamento via uplinks com o empilhamento de switches:

- **Cascateamento (Uplink)**: Conecta switches como dispositivos independentes, cada um com sua própria gerência e sistema operacional. É realizado por meio de portas comuns dos switches, usando cabos par trançado, fibra óptica ou cabos DAC.
- **Empilhamento (Stacking)**: Combina vários switches físicos em uma única entidade lógica, que opera como um único switch gerenciável. Compartilha uma única tabela MAC, um único endereço IP de gerência e simplifica a configuração. Geralmente, oferece maior largura de banda entre os membros do *stack* do que *uplinks* tradicionais. Utiliza cabos proprietários de curta distância, com interfaces e conectores específicos para esta finalidade.

Alguns problemas surgem ao configurar o cascateamento pelas portas do switch devido a limitação da velocidade da porta usada para *uplink*. Ao interligar um switch com outro por uma porta em 1 Gbit/s, a largura de banda disponível na conexão entre os switches será limitada em 1 Gbit/s. Se todas as portas dos switches conectadas em dispositivos estiverem em 1 Gbit/s, haverá um gargalo em caso de tráfego gerado na porta de *uplink*. Outro problema está no ponto único de falha que o uso de apenas uma porta de *uplink* gera. Se esta porta falhar, todos os dispositivos que ficam atrás desta porta ficarão indisponíveis para o resto da rede.

Para resolver estes problemas podem ser usados os recursos do protocolo STP e da agregação de links. Ao conectar várias portas de *uplink* entre dois switches configura-se um *loop*, se todas as portas estiverem ativadas ao mesmo tempo e sem nenhuma configuração adicional. Ao ativar o protocolo STP haverá o bloqueio de portas, onde ficará apenas uma porta ativa. Na Figura 38, um exemplo de uplinks redundantes entre dois switches. Com o STP ativado, duas portas ficariam em estado de bloqueio. Em caso da queda do *uplink* ativo, uma das portas em bloqueio seria escolhida para entrar em estado *Forwarding*, ou seja, ativada para encaminhar pacotes. Este processo com o uso do STP padrão pode levar cerca de 40s, com o uso do RSTP este tempo pode chegar a 10s ou menos. É importante observar que as configurações das portas, VLANs por exemplo, devem estar iguais em todas as portas para não haver indisponibilidades em caso de trocas de portas.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Figura 38. Redundância nos uplinks.

Uma outra solução está no uso de agregação de portas *(link agregation*). No caso da Figura 39, seria configurada uma agregação com um grupo com 3 portas. Este grupo funciona como uma única interface e não configura um *loop* de rede. A partir disto, as 3 portas podem encaminhar pacotes simultaneamente, configurado um *uplink* com 3x mais capacidade, por exemplo, se as portas são de 1 Gbit/s, seria possível encaminhar 3 fluxos de 1 Gbit/s de forma simultânea. Em caso de falha em alguma porta, o grupo de agregação de porta ficará degradado, mas ainda funcional. A desvantagem deste tipo de configuração é o número de portas a serem utilizadas na configuração. Na Figura 39, a configuração de uma interface de agregação em um switch HP modelo 1920s, onde devem ser escolhidas as portas e o algoritmo de balanceamento do tráfego entre as portas. Após a criação da interface de agregação, devem ser configuradas as VLANs na nova interface, com o cuidado das portas físicas que devem estar com as mesmas configurações de velocidade e VLANs para poder formar a agregação com sucesso .

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

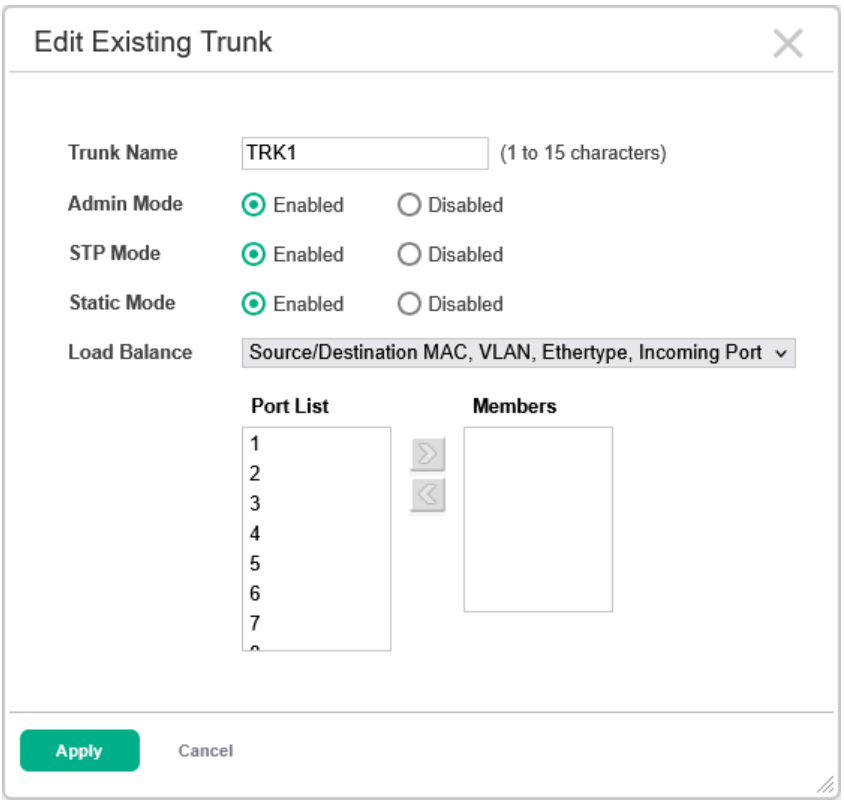


Figura 39. Configuração de agrupamento de portas para agregação (TRUNK na interface do switch HP 1920).

A situação ideal é o uso de portas com maior capacidade para serem utilizadas como porta de *uplink*. Em switches com portas 1 Gbit/s, podem existir uma ou mais portas em 10 Gbit/s para serem utilizadas como *uplinks*. Mesmo nestas situações pode ser utilizada configuração de redundância, com STP ou com agregação, aumentando a segurança e o desempenho da rede. Uma boa prática na administração de cabos de *uplink* é a utilização de cores diferentes nos *patch cords* para fácil identificação da porta em um *rack*.

6.4 Topologia em Anel

A utilização de topologias em anel na interligação de switches em redes locais corporativas não é tão comum. O uso deste tipo de topologia é mais comum em cenários de redes metropolitanas (MAN - *Metropolitan Area Network*) ou em ambientes de provedores para disponibilização de cobertura em uma área geográfica maior. A topologia em anel provê redundância nos caminhos entre switches. Devido ao fechamento dos enlaces em um *loop*, o uso do protocolo STP é necessário ou outro protocolo proprietário com funcionalidades

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

similares tais como o EAPS (*Ethernet Automatic Protection Switching*) da empresa Extreme ou o CSS (*Cluster Switch System*) da empresa Huawei. Desta forma, ao haver a queda de um enlace, a comunicação ficará disponível por outro caminho dentro do anel.

Redes para Iniciantes - Topologias - https://youtu.be/7KXiVKjw6Ko

Na Figura 40, está um exemplo de topologia em anel com 4 switches. Em cenários de tráfego intenso, a necessidade de os dados passarem por múltiplos switches no anel antes de chegarem ao destino pode levar a um desempenho inferior em comparação com uma topologia em estrela onde cada dispositivo tem uma conexão direta com um switch de distribuição ou de *core* (núcleo da rede).

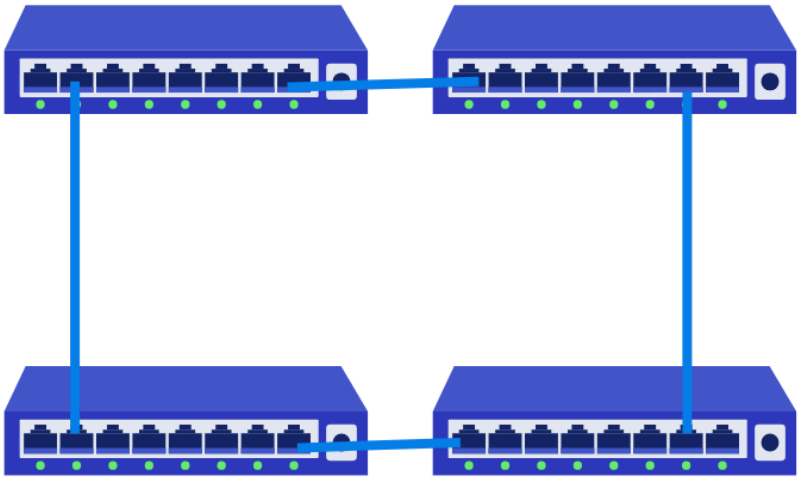


Figura 40. Topologia em anel com uso de STP.

Outra funcionalidade provida pelo protocolo STP é por meio de configurações de custos direcionar o tráfego pelo caminho com melhores recursos e realizar o particionamento do anel para prover maior largura de banda, fazendo com que o tráfego seja enviado por um número menor de switches. O custo de cada interface é baseado na velocidade da porta. Se houver múltiplos links redundantes entre switches com a mesma velocidade, é possível diminuir o custo de um link específico para torná-lo o caminho preferencial. Na Tabela 45 estão exemplos de valores de custo STP associados a diferentes velocidades de porta, baseados nos padrões revisados (IEEE 802.1D-2004/T) que são mais comuns em switches atuais. Estes custos podem ser alterados de forma administrativa no switch para que possa ser definido um caminho de acordo com a necessidade do administrador da rede.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Tabela 45. Custos STP para velocidades de portas

Velocidade da Porta	Custo STP
10 Mbit/s	2.000.000
100 Mbit/s	200.000
1 Gbit/s	20.000
10 Gbit/s	2.000
25 Gbit/s	800
40 Gbit/s	500
100 Gbit/s	200
1 Tbit/s	20

Sobre as VLANs, estas deverão ser configuradas em todos os switches onde o tráfego do anel passar, caso contrário, quando houver uma mudança de topologia com a queda de um enlace, uma ou mais VLANs poderão ficar indisponíveis. Aliado ao aumento da complexidade no diagnóstico de problemas na rede com o uso da topologia em anel, o protocolo STP possui algumas limitações relacionadas à "profundidade" da rede. Em casos onde exista uma grande número de switches cascateados, poderá haver mudanças de topologias do STP constantes que causam sobrecarga de CPU nos dispositivos. Nestes cenários deverá haver ajustes nos temporizadores do STP.

Na Figura 41 está a configuração global do STP em um switch modelo HP 1920. Nesta opção podem ser alterados os temporizadores, custos das interfaces e ativação de proteção de BPDU (para não haver interferência na topologia do STP com mensagens de dispositivos não autorizados). No exemplo da Figura 41 está ativado o MSTP (*Multiple Spanning-Tree*) que atua em instâncias por VLANs e não em uma instância única como no STP. Desta forma, podem ser configurados caminhos diferentes para determinadas VLANs e o tempo de convergência da topologia será otimizado.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

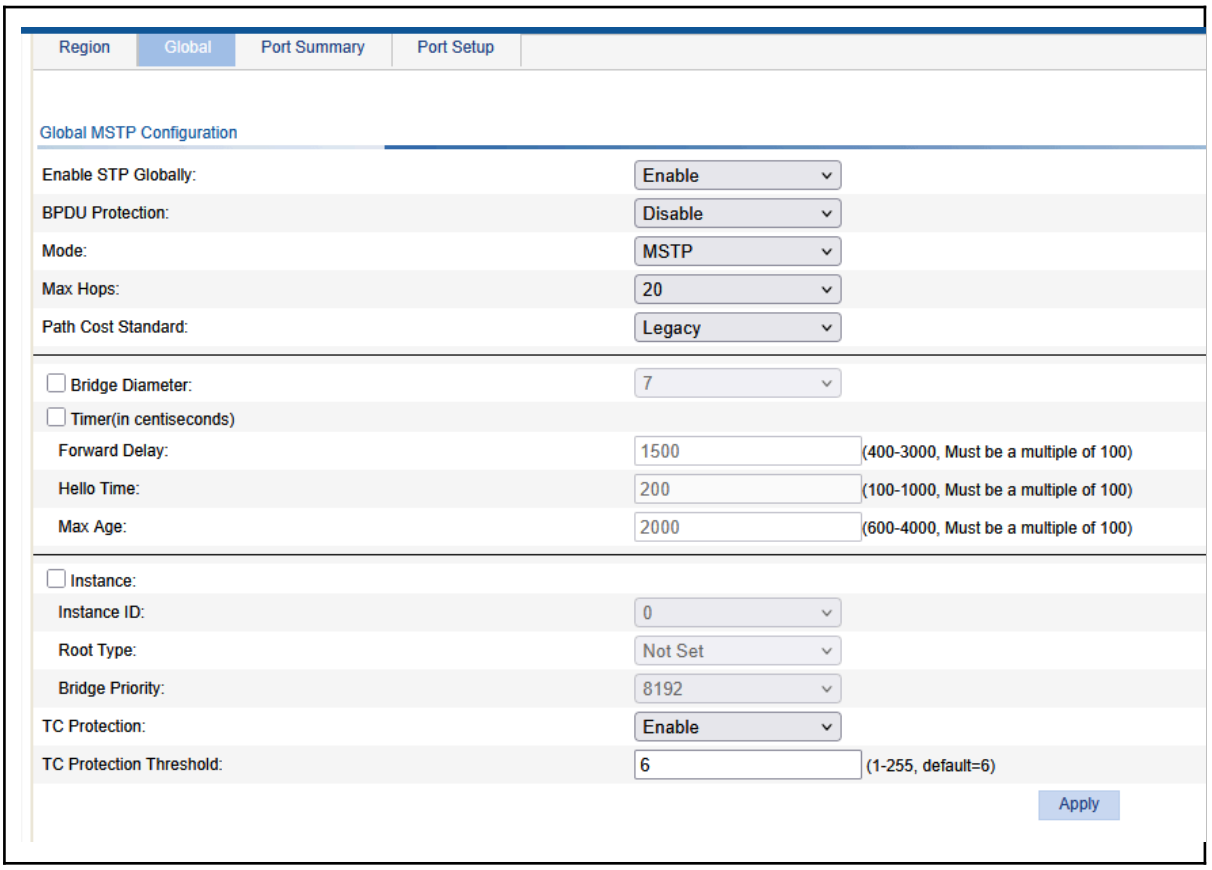


Figura 41. Configuração global do STP em um switch modelo HP 1920.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

7) Resolução de Problemas

A administração de redes, por sua natureza dinâmica e complexa, inevitavelmente apresenta desafios e a necessidade de solucionar problemas de forma rápida e consistente. Este capítulo tem como foco discutir as estratégias e apresentar o conhecimento das ferramentas essenciais para diagnosticar e resolver as ocorrências mais comuns em switches gerenciáveis ambientes de redes locais corporativas. A dica principal para diagnosticar um problema é partir do mais básico e ir escalando até a possibilidade mais complexa. Em muitos casos, um problema de rede pode ser resolvido apenas com a troca de um *patch cord* ou o ajuste de um conector!

Redes para Iniciantes - Testagem de Cabos - https://youtu.be/1ZVR1YjbDsg

Serão abordadas metodologias para a **Busca de Dispositivos** quando estes se tornam inacessíveis ou desconhecidos na rede. Serão apresentadas as causas e soluções para cenários onde uma **VLAN não funciona** como esperado, impactando a comunicação entre segmentos da rede. A identificação e a eliminação de **Loops**, um problema crítico que pode paralisar a rede, receberão atenção detalhada. A análise e a interpretação de **Anomalias** no tráfego e no comportamento dos dispositivos serão exploradas como indicadores de problemas subjacentes. O processo de **Adição de Novos Dispositivos** à rede e a resolução de potenciais conflitos de configuração serão discutidos.

Serão apresentadas **Ferramentas de Gerenciamento** que auxiliam no diagnóstico e na resolução de problemas, oferecendo visibilidade e controle sobre a infraestrutura de rede. Os **Ambientes de Simulação e Emulação** são úteis para explorar as funcionalidades dos switches e realizar testes em configurações e cenários. Finalmente, serão compiladas **Boas Práticas** para a prevenção de problemas e para a implementação de uma abordagem sistemática na resolução de incidentes.

7.1 Busca de Dispositivos

Para descobrir dispositivos na rede pode-se utilizar as funcionalidades de buscas por endereços físicos na tabela MAC ou utilizar o protocolo de descoberta LLDP (*Link Layer Discovery Protocol*). Para o caso de busca por endereços físicos é importante saber previamente o endereço do dispositivo ou, ao menos, o fabricante do dispositivo que é

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

identificado pelos 3 primeiros bytes do endereço MAC. Por meio do prefixo do endereço que identifica o fabricante, poderá ser uma informação valiosa para descobrir um dispositivo se for um caso onde é um dispositivo incomum conectado na rede. Por exemplo, um prefixo de endereço MAC da empresa Alcatel, fabricante de equipamentos VoIP, ou da empresa Lexmark, fabricante de impressoras, poderá ajudar na descoberta dos dispositivos conectados nos switches. Outro fator importante é saber em qual VLAN o dispositivo deveria estar. Se estiver documentada a VLAN na qual o dispositivo deveria estar conectado, a busca seria reduzida para apenas portas configuradas na VLAN de interesse.

A tabela de endereços MAC (*MAC Address Table* ou *CAM Table*) fica armazenada na memória do switch e é dinâmica. Nesta tabela o switch mantém uma listagem que associa endereços MAC a portas físicas. A forma de acesso da tabela poderá variar bastante de um switch para outro, inclusive com alterações no formato do endereço físico que deverá ser informado para a busca. Os formatos podem variar em relação aos agrupamentos de 6 bytes que formam o endereço. O formato mais comum é o de cada byte separado pelo caractere ":", por exemplo 00:AB:CD:EF:01:02. Entretanto, formato separados por hífens, 00-AB-CD-EF-01-02, ou por ponto em agrupamentos de 2 bytes, 00AB.CDEF.01:02 ou 00AB-CDEF-01:02, e em alguns casos a interface de gerenciamento aceita qualquer formato. Na Figura 43 está um exemplo da interface de gerenciamento do switch Aruba modelo 1930 com as opções de buscas na tabela MAC para a VLAN 3333 e prefixo de MAC 00:0b:82 (00:0B:82 *Grandstream Networks, Inc.*). Está disponível no site https://www.wireshark.org/tools/oui-lookup.html um serviço de busca para identificar os prefixos dos fabricantes.

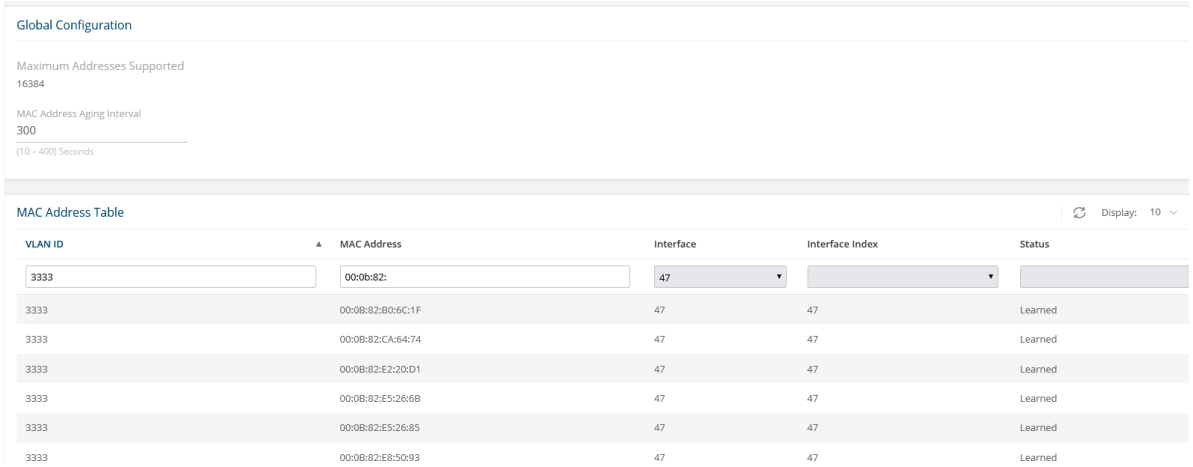


Figura 43. Tabela MAC no switch Aruba modelo 1930

Os protocolos de descoberta de camada 2 são protocolos tais como CDP (*Cisco Discovery Protocol*) e LLDP (*Link Layer Discovery Protocol*) que permitem que dispositivos

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

vizinhos se anunciem uns aos outros. Ao habilitar esses protocolos nos switches, é possível visualizar informações sobre os dispositivos diretamente conectados, incluindo seus endereços MAC, endereços IP (se disponíveis), nome do dispositivo, interface local e interface vizinha. O uso mais comum do LLDP é para descoberta de switches conectados diretamente. Desta forma, é possível saber as conexões de *uplink* entre os switches e saber informações diversas. Outros dispositivos que fazem anúncios por LLDP são telefones IP, roteadores e *access points*. As implementações do protocolo LLDP não estão restritas a dispositivos de rede e podem ser ativadas em sistemas operacionais Windows e Linux. O objetivo disto é localizar o switch que está fazendo a conexão dos computadores e para saber em qual porta física do switch está sendo utilizada. Na Figura 44 o cliente de LLDP para Windows LDWin (https://github.com/chall32/LDWin) ativado em um computador com o sistema operacional Microsoft Windows 11.

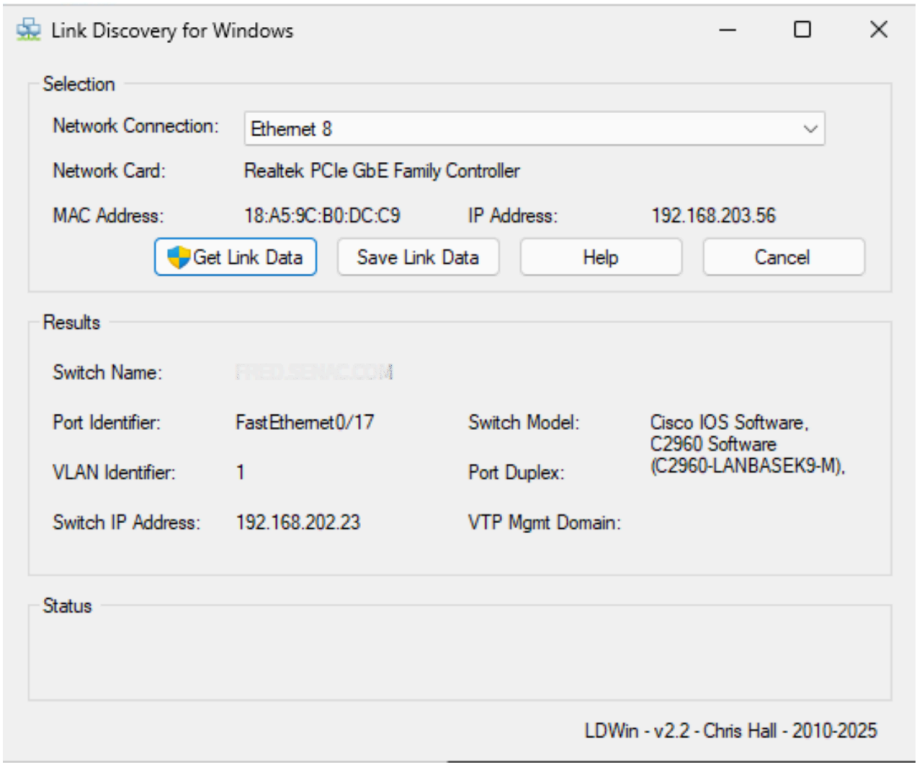


Figura 44. Execução do cliente de LLDP LDWin

Outra informação relevante com o uso do LLDP em computadores é identificar em qual VLAN um determinado dispositivo está conectado. Esta informação não é simples de obter estando do lado do cliente. Para verificar os vizinhos em um switch Cisco pode-se utilizar o comando *show lldp neighbors detail*. Em interface gráfica as consultas podem ser realizadas na funcionalidade LLDP disponível na console web dos switches. Na Figura 45, um

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

exemplo da saída da execução de um comando para listar os vizinhos de um switch Huawei modelo S5720.

```
<SW_DATACENTER_CISCO>display lldp neighbor brief
Local Intf       Neighbor Dev            Neighbor Intf           Exptime(s
GE0/0/1          ucs-anglo-A             Eth1/4                  109
GE0/0/2          ucs-anglo-A             Eth1/3                  109
GE0/0/3          ucs-anglo-B             Eth1/4                  109
GE0/0/4          ucs-anglo-B             Eth1/3                  109
XGE0/0/1         DC_Anglo_Rack5_Data2    XGE0/0/1                103
<SW_DATACENTER_CISCO>
```

Figura 45. Listagem de vizinhos LLDP em um switch Huawei modelo S5720

A ativação do protocolo LLDP é opcional e não é comum e nem desejável que seja ativado em portas de acesso conectadas com dispositivos de usuários. O uso mais comum é em portas de *uplink* para identificação de switches vizinhos. Existem switches mais antigos que não possuem o LLDP e desta forma não serão descobertos nas portas de um switch que tenha o protocolo ativado. Portanto, para o LLDP funcionar, ambos dispositivos conectados devem possuir o protocolo ativado.

7.2 VLAN não funciona

Em casos onde um dispositivo associado a uma VLAN em um switch não aparece em outro switch conectado algumas validações e procedimentos devem ser realizados para identificar a origem do problema. Um dos casos mais comuns é a falta da VLAN associada em portas em algum switch entre a origem e o destino. A primeira verificação é checar a existência da VLAN, com o VID (*VLAN ID*) correto, em todos os switches entre a origem e o destino. A partir desta confirmação, verificar se as portas de *uplink* entre os switches possuem a VLAN nos dois lados da conexão. Em caso de portas *trunk*, a VLAN poderá ser configurada como marcada (*tagged*), forma mais comum, ou desmarcada (*untagged*). Na porta do outro lado do *uplink* as configurações de marcada e desmarcada devem combinar. Outra verificação importante é a porta onde está o dispositivo de destino, se está associada a VLAN com a marcação correta. Se for um dispositivo final, tal como um computador de usuário, a VLAN deve estar associada como desmarcada devido ao dispositivo não tratar as *tags* de VLAN. Na checagem de conexões físicas de forma remota, deve-se verificar se as portas corretas estão sendo usadas. Uma das formas de verificar isto é verificando no logs o tempo de atividade da porta, os endereços MAC que aparecem associados nas portas e as configurações existentes no switch que podem indicar qual o uso da porta.

Com o endereço MAC do dispositivo final é possível verificar as tabelas de endereços MAC nos switches e realizar buscas para saber em qual VLAN o MAC do dispositivo aparece.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Na Figura 46, um exemplo de busca pelo endereços físico *5c:d9:98:a0:e1:8f* na VLAN com identificação 180 em um switch Extreme modelo X460.

```
SW_COMEP_[redacted].9 # show fdb vlan 180 | grep 5c:d9:98:a0:e1:8f
VLAN 180: show fdb vlan vigilancia | grep 5c:d9:98:a0:e1:8f
5c:d9:98:a0:e1:8f vigilancia(0180) 0104  d m           19
SW_COMEP_[redacted].10 #
```

Figura 46. Busca por MAC na VLAN 180 em um switch Extreme modelo X460

Se tudo estiver correto, o dispositivo deverá aparecer nas portas de *uplink* em todos os switches entre origem e destino na VLAN esperada. Caso isto não aconteça, deverá ser feito todo o percurso do switch conectado no dispositivo de origem até o switch que conecta o dispositivo de destino, fazendo a checagem básica de configurações, tipos de portas e buscas na tabela MAC de cada switch. Outros motivos que podem gerar problemas para o funcionamento correto de VLANs estão listados na Tabela 46.

Tabela 46. Outros motivos para o não funcionamento de VLANs

Motivo	Causas Prováveis
Configuração Incorreta das Portas	• **Porta no modo de acesso incorreto:** Se um dispositivo final (como um computador) que deveria estar em uma VLAN específica estiver conectado a uma porta configurada para outra VLAN (ou para a VLAN nativa incorreta), ele não conseguirá se comunicar com outros dispositivos na VLAN desejada. A porta precisa estar configurada como acesso para a VLAN correta • **Porta trunking mal configurada:** Em links de tronco (*trunk*) a configuração das VLANs permitidas pode estar incorreta. Se uma VLAN específica não estiver permitida no tronco, o tráfego dessa VLAN não passará por esse enlace • **VLAN nativa incompatível:** Em links de tronco, ambos os lados da conexão devem ter a mesma VLAN nativa configurada. O tráfego não marcado que passa no tronco é associado à VLAN nativa. Se houver incompatibilidade, pode haver problemas de comunicação para esse tráfego não etiquetado e até mesmo para o tráfego etiquetado

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Problemas de Tagging (Etiquetamento) de VLANs	• **Dispositivo final não suporta *tagging*:** Dispositivos finais (PCs, servidores) geralmente não etiquetam o tráfego com informações de VLAN. Eles esperam estar em uma porta de acesso configurada para a VLAN correta. Se um dispositivo que não suporta *tagging* for conectado a uma porta *trunk*, a comunicação falhará • **Erro na configuração do *tagging* em servidores ou dispositivos especiais:** Alguns servidores ou dispositivos de rede (como firewalls ou roteadores) podem precisar ser configurados para etiquetar o tráfego com informações de VLAN. Uma configuração incorreta nesse ponto impedirá a comunicação com a VLAN desejada
Incompatibilidade ou Erros de Configuração entre Switches	• **VLAN não criada em todos os switches:** Uma VLAN precisa ser criada em todos os switches pelos quais o tráfego dessa VLAN precisa passar. Se uma VLAN existir em um switch, mas não em outro no caminho da comunicação, o tráfego será descartado. • **Erros de Spanning-tree (STP):** Embora o STP seja projetado para evitar *loops*, configurações incorretas podem bloquear portas que deveriam estar encaminhando tráfego para uma determinada VLAN. Isso pode isolar segmentos da rede. • **Configurações de VLAN *pruning* incorretas:** O VLAN *pruning* (eliminação de VLANs) é usado para otimizar o tráfego em links de tronco, impedindo que VLANs desnecessárias sejam transmitidas por um link. Se o *pruning* estiver configurado incorretamente, uma VLAN necessária pode ser bloqueada em um tronco
Problemas de Roteamento Inter-VLAN	• **Roteamento inter-VLAN não configurado:** Para que dispositivos em VLANs diferentes se comuniquem, o roteamento inter-VLAN precisa estar configurado em um roteador ou em um switch *Layer 3*. Se essa configuração estiver ausente ou incorreta, a comunicação entre as VLANs falhará. • **Interfaces de roteamento inter-VLAN inativas ou mal configuradas:** As interfaces virtuais (SVIs) criadas nos

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

	switches *Layer 3* para representar as VLANs precisam estar ativas e com endereçamento IP correto para atuar como *gateways* para os dispositivos nas respectivas VLANs. • **Problemas de roteamento no dispositivo inter-VLAN:** Pode haver problemas com as tabelas de roteamento ou com as políticas de roteamento no roteador ou switch *Layer 3* responsável pelo roteamento entre as VLANs.
Problemas Físicos ou de Camada 1	• **Cabos desconectados ou com problemas:** Uma conexão física defeituosa pode obviamente impedir qualquer comunicação, incluindo o tráfego de VLANs. • **Problemas de velocidade/duplex:** Configurações incorretas de velocidade e duplex podem causar colisões e erros, afetando a comunicação dentro de uma VLAN ou entre VLANs.
Outras Configurações Incorretas	• **Listas de controle de acesso (ACLs) bloqueando o tráfego:** ACLs configuradas incorretamente em switches ou roteadores podem estar bloqueando o tráfego entre dispositivos na mesma VLAN ou entre VLANs diferentes. • **Problemas com protocolos de descoberta (como CDP ou LLDP):** Embora não diretamente causem a falha de uma VLAN, ausência ou problemas com esses protocolos podem dificultar o diagnóstico e a identificação da topologia da rede, tornando a solução de problemas mais complexa.

7.3 Loops

Os loops de rede são um transtorno para qualquer administrador e podem paralisar uma rede inteira. Entender suas causas e como combatê-los é fundamental. Existem dois tipos principais de loops: os de roteamento e os de nível físico/enlace. Os loops de roteamento ocorrem quando há inconsistências nas tabelas de roteamento dos roteadores, fazendo com que pacotes sejam encaminhados indefinidamente. É importante ressaltar que os campos TTL (*Time to Live*) no IPv4 e Hop Limit no IPv6 *não evitam loops*; eles apenas descartam pacotes que excedam um número máximo de saltos, impedindo que circulem eternamente e consumam recursos. A prevenção de loops de roteamento passa pela correta

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

configuração das tabelas de roteamento e pela implementação de protocolos de roteamento dinâmico eficientes.

Os loops no nível físico e de enlace são mais comuns em ambientes de rede local e geralmente resultam de conexões de cabeamento incorretos, criando um caminho circular para os dados. Esses loops causam as chamadas tempestades de broadcast e multicast *(broadcast/multicast storm*).

- **Broadcasts:** Pacotes de broadcast são direcionados a todas as portas da mesma VLAN de um switch. Em um *loop*, um pacote broadcast pode ser replicado e reenviado inúmeras vezes, saturando a rede.
- **Multicasts:** Se o recurso de *IGMP Snooping* não estiver habilitado, pacotes multicast se comportam de forma semelhante aos broadcasts, espalhando-se por toda a VLAN.

As tempestades de broadcast e multicast resultam em um volume de tráfego massivo que consome a largura de banda dos enlaces, tornando a rede muito degradada ou indisponível enquanto durar o loop. Como estratégias para combater o efeito do *loop* na rede existem funcionalidades em switches gerenciáveis e procedimentos que podem ser aplicados na administração da rede que são:

- **Limitação de Pacotes de Broadcast e Multicast**
  - Configurar um limite de pacotes de broadcast e multicast nas portas de acesso dos switches. Um valor de **50 pps (pacotes por segundo)** é um bom ponto de partida para portas conectadas a dispositivos comuns como computadores, impressoras ou *Access Points* (APs) em modo roteador. Isso ajuda a conter tempestades antes que se espalhem. Na Figura 47, exemplo de configuração dos limites de broadcast e multicast para 50 pacotes por segundo em uma interface no switch HP modelo 1920s.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

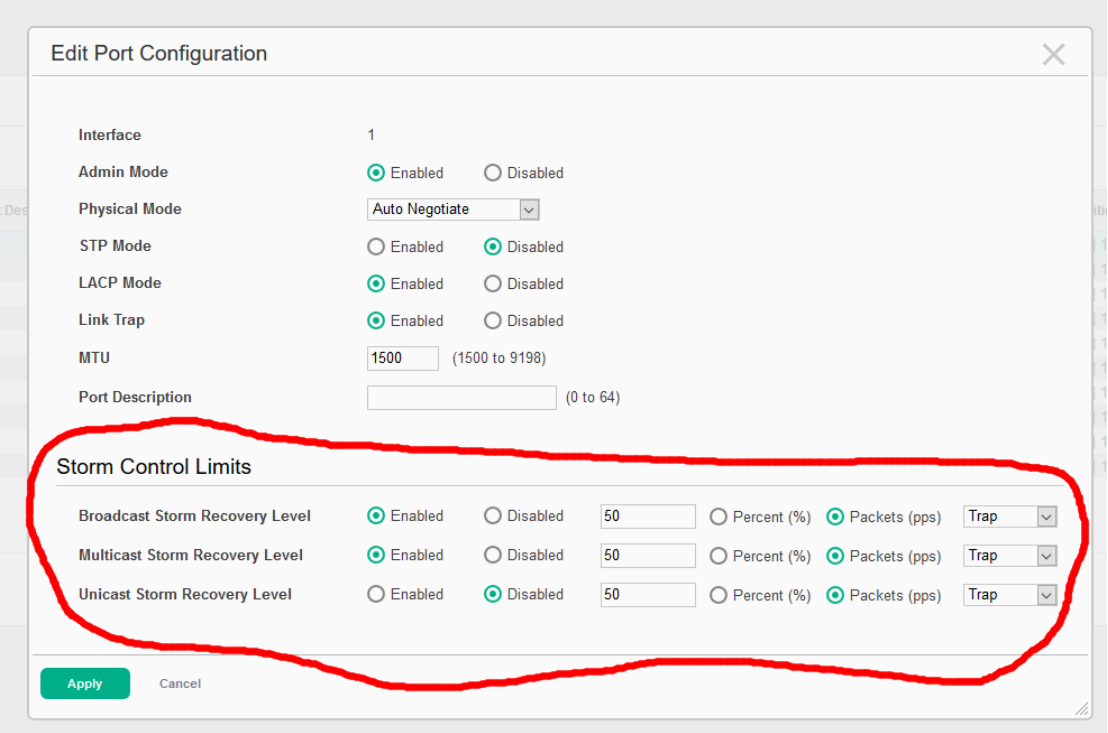


Figura 47. Limitação de 50pps em uma porta de um switch HP modelo 1920s.

- **Ativação do Protocolo STP (Spanning-Tree Protocol)**
  - O STP (*Spanning-Tree Protocol)* é essencial. Ele cria uma topologia lógica livre de *loops*, bloqueando portas redundantes. É altamente recomendável usar a versão RSTP (*Rapid Spanning-Tree Protocol*) devido à sua convergência mais rápida. Configurar o switch raiz (*root bridge*) para o *core* da rede para otimizar o fluxo de dados. É importante ressaltar que o STP não resolve um loop em dispositivos que não o suportam.
- **Organização e Documentação do Cabeamento**
  - Uma organização e documentação impecável do cabeamento e dos racks são medidas simples, mas extremamente eficazes. Manter o cabeamento organizado reduz significativamente a chance de erros que geram *loops* físicos.
- **Ativação do *Loop Protection***
  - O recurso de *Loop Protection* nas portas dos switches é um dos procedimentos mais eficazes para evitar a propagação de tráfego de loops. Ele permite bloquear automaticamente as portas que detectam a formação de um loop, isolando o problema e protegendo o restante da rede. É especialmente útil quando os dispositivos conectados a essas portas não possuem funcionalidades de STP.
- **Segmentação da Rede com VLANs**

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- O uso de VLANs é fundamental para segmentar a rede e diminuir o impacto dos loops. Ao separar os domínios de broadcast, um *loop* em uma VLAN afetará apenas essa VLAN, e não a rede inteira. Além disso, a origem do loop pode ser descoberta mais rapidamente. Entretanto, mesmo com o uso de VLAN separadas, se uma VLAN com *loop* estiver sendo passada em uma porta tronco este enlace ficará degradado e causará impacto em outras VLANs que estejam na mesma porta tronco.

- **Definição de Políticas de Uso da Rede**
  - Estabelecer políticas claras sobre o uso de equipamentos na rede e conscientizar os usuários sobre os riscos de conectar APs, switches ou qualquer outro dispositivo sem o conhecimento da área de TI é essencial para evitar loops não intencionais.
- **Desabilitação de Portas Não Utilizadas**
  - Desabilitar as portas do switch que não estão em uso é uma prática de segurança e prevenção. Isso diminui as chances de alguém criar um loop físico acidentalmente entre tomadas de rede ou conectar equipamentos não autorizados. Na Figura 48, um exemplo comum de risco potencial para *loop* com uma tomada dupla de rede, onde a simples conexão de um *patch cord* entre elas configura um *loop* físico.

Figura 48. Tomada de rede dupla que pode ser a origem de um loop físico de rede.

- **Limitação da Velocidade das Interfaces de Usuário**
  - Limitar a velocidade das interfaces de rede para os usuários pode mitigar o impacto de um *loop*. Um *loop* em uma interface de 1 Gbit/s causará muito mais estrago do que em uma de 10 Mbit/s. Para acesso à internet, por exemplo, 100 Mbit/s, até mesmo 10 Mbit/s, geralmente é mais do que suficiente para um usuário comum.
- **Ativação de DHCP Snooping**

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

    - A funcionalidade de DHCP Snooping bloqueia o tráfego de DHCP não autorizado, prevenindo que APs "piratas" (*rogue APs*) e roteadores não homologados causem não apenas *loops*, mas também outros problemas de conectividade e segurança na rede.
- **Uso de Ferramentas de Gerenciamento de Rede**
    - Utilizar ferramentas de administração de redes como Nagios (https://www.nagios.org/), Observium (https://www.observium.org/), Zabbix (https://www.zabbix.com/) ou MRTG (https://github.com/oetiker/mrtg) é indispensável. Elas permitem monitorar os dispositivos e o tráfego, identificar anomalias e atuar proativamente na detecção e resolução de loops.

Os *loops* causam transtornos significativos para todos os usuários e, principalmente, para os administradores de rede. A utilização de switches gerenciáveis e de ferramentas de gerenciamento de rede, configurados corretamente, e organização do cabeamento são as principais formas de reduzir o impacto dos loops. As medidas mais imediatas a serem aplicadas em switches são a ativação do *Loop Protection* e a limitação de pacotes de Broadcast/Multicast nas portas.

7.4 Anomalias

É uma boa prática na administração de redes investigar qualquer alteração ao comportamento padrão de um dispositivo, sistema, aplicação ou tráfego de pacotes. Com o uso de ferramentas de monitoramento torna-se possível gerar um *baseline* (padrão) do comportamento da rede. No caso de switches gerenciáveis algumas anomalias, que são desvios do comportamento padrão, acontecem em casos tais como consumo elevado de tráfego nas portas, portas com alterações de estado (*flapping*), endereços MAC flutuantes, configurações de *duplex* e velocidade da porta incorretos, lentidão no acesso ao switch por motivo de alto consumo de CPU e erros de pacotes em portas. Para possibilitar a descoberta das causas dessas anomalias podem ser realizados os seguintes procedimentos e análises:

- **Descartes e erros de pacote:** Um aumento significativo no número de pacotes descartados ou erros em uma interface podem indicar problemas físicos (como cabeamento defeituoso), incompatibilidade de velocidade/duplex ou sobrecarga. Se uma porta estiver a 10 Mbit/s em Half-Duplex pode ser problema físico no cabo e a Auto Negociação não ocorreu corretamente.
- **Latência incomum:** Um aumento na latência (tempo de resposta) para o tráfego que passa pelo switch pode indicar congestionamento, problemas de qualidade de serviço (QoS) mal configurados ou um switch com alto consumo de processamento.
- ***Flapping* de porta:** Uma interface que alterna repetidamente entre os estados *up* (ativo) e *down* (inativo) geralmente indica um problema físico com o cabo, o conector

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-Compartilhalgual 4.0 Internacional

ou o próprio dispositivo conectado. Este comportamento pode estar relacionado ao modo de economia de energia ativada ou dispositivo em modo suspenso.

- **Perda de conectividade inesperada:** Dispositivos que perdem a conectividade repentinamente e de forma intermitente podem indicar problemas com a porta do switch, alterações na VLAN configurada ou problemas na configuração do protocolo STP.
- **Falhas no *Spanning Tree Protocol* (STP):** Mudanças inesperadas na topologia do STP, *loops* detectados ou portas bloqueadas incorretamente podem causar interrupções temporárias ou até mesmo permanentes em portas ou em VLANs.
- **Problemas com agregação de links (LAG/EtherChannel):** Falhas em um ou mais membros de uma agregação, levando à redução da largura de banda ou perda de redundância, são anomalias.
- **Tráfego incomum:** Padrões de tráfego que não correspondem ao comportamento normal da rede, tais como picos de tráfego em horários incomuns, podem indicar uma intrusão ou um dispositivo comprometido.
- **Violações de segurança de porta:** Detecções de violações de segurança de porta, por exemplo, muitos endereços MAC em uma única porta configurada com *port security* com limitação de número de MAC, indicam tentativas de acesso não autorizado.
- **Tentativas de login na console de administração:** Um número excessivo de tentativas de login na console de administração de um switch pode indicar uma tentativa de ataque de força bruta ou algum *script* de automação com senhas desatualizadas.
- **Alterações de configuração não autorizadas:** Qualquer modificação na configuração do switch que não foi realizada por um administrador autorizado é uma anomalia de segurança grave. Importante manter backup das configurações e limitar as permissões de acesso no switch.
- **Reinicializações inesperadas:** Um switch que reinicia sem intervenção manual indica um problema de *hardware* ou *software* crítico. Deve-se monitorar o *uptime* do switch para verificar se estão havendo reinicializações.
- **Falhas de energia:** Problemas com a fonte de alimentação, levando à perda de energia ou comportamento instável. Devido ao tempo necessário para voltar ao estado operacional em um switch gerenciável, deve-se manter o fornecimento de energia ininterrupto em racks de comunicação com o uso de nobreaks.
- **Problemas de Syslog/SNMP:** Falha no envio de logs para o servidor de logs remoto ou respostas inesperadas do SNMP por meio de *Traps* podem indicar problemas de configuração ou falhas no switch.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Alertas do sistema:** Mensagens de erro ou avisos de alertas gerados na console pelo próprio switch indicam condições anormais que precisam ser investigadas.

7.5 Adição de Novos Switches

Ao adicionar um novo switch na rede deve-se verificar se há instalação elétrica disponível no rack, espaço suficiente e compatível com a profundidade do novo switch. Em caso de não ser compatível com as dimensões do rack ou não ter espaço livre, alterações deverão ser realizadas, com a provável troca do rack por um com maior tamanho para comportar o novo switch. Portanto, utilizar a recomendação de dimensionar 40% do espaço livre de ocupação no rack é uma medida importante e será benéfica no futuro. Outros procedimentos necessários são a configuração do novo switch e a instalação física no rack. A instalação física poderá causar indisponibilidade na rede em caso de necessidade de desligamento do rack para acomodar o novo dispositivo.

Além disso, deverá haver porta disponível no switch que proverá o *uplink* para o novo switch. Com a necessidade de expansão da rede, poderá ser necessária a substituição de um switch por outro com mais portas, por exemplo a troca de switch de 24 para 48 portas, ou adição de um novo switch no rack. Para evitar problemas na adição de novos switches na infraestrutura de rede existente algumas medidas são necessárias:

Planejamento Prévio:

- **Análise da Necessidade:** Antes de adquirir um novo switch, avaliar cuidadosamente as necessidades. Considerar o número de novas conexões, a largura de banda exigida, os requisitos de VLAN e quaisquer funcionalidades específicas tais como PoE, *uplinks* de alta velocidade e enlace de fibra óptica.
- **Compatibilidade:** Verificar a compatibilidade do novo switch com os switches existentes na rede, incluindo protocolos de gerenciamento (SNMP), protocolos de roteamento (se aplicável), e funcionalidades como STP e VLAN. Em caso de funcionalidades proprietárias como *clustering* para gerenciamento ou empilhamento devem ser adquiridos switches de mesmo fabricante e modelo.
- **Topologia da Rede:** Planejar a melhor localização física e a forma de interconexão do novo switch com a topologia existente. Considerar a redundância de links e os caminhos de tráfego.
- **Endereçamento IP:** Definir um endereço IP de gerenciamento para o novo switch que esteja dentro do esquema de endereçamento e não cause conflitos.
- **Configuração Inicial:** Ter um plano para a configuração inicial do switch, incluindo nome do host, senha administrativa, configuração de VLANs básicas e configurações

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

de *uplink*. Importante nesta etapa possuir um modelo (*template*) com as configurações básicas que são padrão nos switches já existentes na rede.

Configuração Prévia (*Staging*):

- **Ambiente Isolado:** Se possível, configurar o novo switch em um ambiente isolado (*staging*) antes de conectá-lo à rede de produção. Isso permite testar a configuração básica, atualizar o *firmware* e verificar a funcionalidade sem afetar a rede ativa.
- **Atualização de Firmware:** Verificar se há atualizações de *firmware* disponíveis para o novo switch e realizar a atualização antes de colocá-lo em produção. Os *firmwares* atualizados geralmente contêm correções de *bugs* e melhorias de segurança.
- **Configuração Básica:** Configurar o nome do host, o endereço IP de gerenciamento, o *gateway* padrão, as configurações de DNS e as credenciais de acesso administrativo (senha forte). A configuração para o uso de *gateway* não é obrigatória se a VLAN de administração dos dispositivos está configurada nas estações e servidores de gerenciamento.
- **VLANs e Trunking:** Configurar as VLANs que serão utilizadas no novo switch e as portas de tronco (*trunk*) necessárias para a comunicação com outros switches. Verificar se as VLANs permitidas nos troncos estão corretas e se o padrão nomes e identificações das VLANs correspondem com o restante do switches.
- ***Spanning Tree Protocol* (STP):** Configurar as prioridades de STP no novo switch, especialmente se ele for fazer parte da topologia STP existente. Uma configuração inadequada pode causar a escolha errada do switch raiz, *loops* ou problemas de convergência.

Conexão à Rede:

- **Conexão Gradual:** Conectar o novo switch à rede de produção de forma gradual, começando com as conexões de *uplink*. Monitorar o comportamento da rede após cada conexão.
- **Verificação de Loops:** Antes de conectar dispositivos finais ao novo switch, verificar se não há loops na rede causados pela adição do novo equipamento. Monitorar o tráfego de broadcast e multicast nas interfaces do switch para identificar alguma anomalia.
- **Testes de Conectividade:** Após conectar os dispositivos finais, realizar testes de conectividade para garantir que eles consigam se comunicar com outros dispositivos na mesma VLAN e em VLANs diferentes (se o roteamento inter-VLAN estiver envolvido).
- **Monitoramento:** Ativar o agente SNMP e adicionar o novo switch na ferramenta de gerenciamento. Monitorar de perto o desempenho do novo switch e o impacto na

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

rede utilizando as ferramentas de gerenciamento disponíveis. Verificar a utilização da CPU, da memória e das interfaces.

Documentação:

- **Atualização da Documentação:** Após a adição bem-sucedida do novo switch, atualizar a documentação da rede, incluindo diagramas de topologia, inventário de hardware e informações de configuração. Importante destacar na documentação as particularidades do switch, por exemplo, os procedimentos para acesso a console de gerenciamento e a restauração das configurações de fábrica. Realizar um backup da configuração assim que estiver completa a instalação do switch.

Considerações de Segurança:

- **Políticas de Segurança:** Aplicar as mesmas políticas de segurança utilizadas nos outros switches ao novo equipamento, tais como configuração de SNMP seguro (SNMPv3), controle de acesso administrativo (ACLs), usuários e senhas padrão e desativação de serviços desnecessários.
- **Realizar Auditoria de Segurança:** Executar rotinas de busca de vulnerabilidades no novo switch para detectar possíveis falhas de segurança. Aplicar as recomendações de segurança providas pela documentação do fabricante do switch.

Capacidade e Escalabilidade:

- **Margem de Crescimento:** Ao adicionar um novo switch, considerar a capacidade futura da rede e escolher um equipamento que ofereça alguma margem para crescimento. Em alguns modelos de switches é possível realizar o empilhamento virtual com o uso de *clustering*. Em caso de uso de switches empilháveis verificar o limite de empilhamento do modelo escolhido. Outro requisito importante é para expansão de enlace ópticos com portas SFP e suas variações. A falta deste tipo de porta poderá forçar a troca de um switch por outro com maior número de portas em um curto prazo de tempo, em caso de falha no planejamento.

7.6 Ferramentas de Gerenciamento

A complexidade das redes locais corporativas torna a administração manual de switches gerenciáveis uma tarefa quase impraticável em ambientes de médio a grande porte. Nestes casos as ferramentas de gerenciamento de rede se tornam aliadas indispensáveis. Elas automatizam e simplificam processos críticos, como a descoberta de dispositivos, o

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

mapeamento da topologia, a configuração em massa, o monitoramento contínuo e a análise de desempenho.

A principal vantagem do uso dessas ferramentas reside na otimização da rotina do administrador de redes. Elas fornecem uma visão centralizada e granular da infraestrutura, permitindo identificar gargalos, prever falhas e garantir a segurança das portas. Com recursos de alerta proativo, é possível ser notificado sobre anomalias antes que se transformem em problemas maiores, minimizando o tempo de inatividade da rede.

Para a resolução de problemas, a importância dessas ferramentas é inquestionável. Elas permitem que o administrador possa acessar logs detalhados, visualizar estatísticas de tráfego em tempo real, isolar portas com comportamento suspeito, e até mesmo executar diagnósticos remotos. Seja para identificar um *loop* de rede, um problema de desempenho em uma VLAN específica ou uma porta com consumo excessivo, a capacidade de coletar e analisar dados de forma eficiente é fundamental para um diagnóstico rápido e preciso, reduzindo drasticamente o tempo necessário para retornar a normalidade (MTTR (*Mean Time To Restore*)) do switch.

Existem ferramentas proprietárias, com uso restrito para dispositivos de um único fabricante, ferramentas comerciais compatíveis com diversos fabricantes e de código-fonte aberto que podem ser aplicadas em qualquer ambiente. A escolha por uma ou mais ferramentas depende do ambiente que será monitorado. É bastante comum o uso de mais de uma ferramenta para a administração de switches gerenciáveis. O protocolo SNMP é o principal recurso utilizado pelas ferramentas para administração de switches gerenciáveis. Alguns exemplos de ferramentas proprietárias, comerciais e de código-fonte aberto são:

Ferramentas de Gerenciamento Proprietárias

Estas ferramentas são desenvolvidas pelos próprios fabricantes do switch, garantindo total compatibilidade e otimização para seus equipamentos.

- **Cisco DNA Center:** Uma plataforma de gerenciamento de rede empresarial da Cisco, oferecendo automação, análise e *insights* para infraestrutura Cisco, disponível em https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html
- **HPE Aruba Central:** Solução de gerenciamento de rede baseada em nuvem da HPE Aruba, para gerenciamento de switches, access points e roteadores Aruba, disponível em https://www.arubanetworks.com/products/network-management/aruba-central/

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Juniper Mist Cloud:** Plataforma de gerenciamento em nuvem da Juniper Networks, utilizando inteligência artificial para automação e insights em redes Juniper, disponível em https://www.mist.com/
- **Dell EMC OpenManage Network Manager:** Ferramenta para gerenciar dispositivos de rede Dell EMC, oferecendo configuração, monitoramento e relatórios. Geralmente, o acesso e *download* de software Dell EMC são feitos via portal de suporte. Buscar por "*OpenManage Network Manager*" em https://www.dell.com/support
- **Huawei eSight:** Plataforma de gerenciamento de rede da empresa Huawei, suportando uma ampla gama de dispositivos Huawei. Similar à ferramenta eNSP, o acesso ao eSight geralmente requer uma conta no portal de suporte da Huawei Enterprise. Buscar por "eSight" em https://support.huawei.com/enterprise/
- **TP-Link tpNMS:** Sistema de gerenciamento de rede da TP-Link, para gerenciar seus switches e outros dispositivos, disponível em https://www.tp-link.com/br/business-networking/management-system/tpnms/
- **Netgear ProSAFE Network Management System (NMS300):** Software para gerenciamento de dispositivos de rede Netgear, incluindo switches, disponível em https://www.netgear.com/business/solutions/network-management/

Ferramentas de Gerenciamento de Terceiros

Estas soluções oferecem suporte a equipamentos de múltiplos fabricantes, sendo ideais para ambientes heterogêneos.

- **SolarWinds Network Performance Monitor (NPM):** Uma ferramenta para monitoramento de desempenho de rede, incluindo switches. Oferece recursos de descoberta, mapeamento, alertas e relatórios, disponível em https://www.solarwinds.com/network-performance-monitor
- **Paessler PRTG Network Monitor:** Uma solução de monitoramento unificada que suporta SNMP, permitindo o monitoramento detalhado de switches de diversos fabricantes, disponível em https://www.paessler.com/prtg
- **ManageEngine OpManager:** Um software de gerenciamento de rede abrangente que oferece monitoramento de switches, servidores, tráfego e muito mais. Inclui um "*Switch Port Mapper*" para visibilidade das conexões, disponível em https://www.manageengine.com/network-monitoring/
- **Datadog Network Monitoring:** Uma plataforma de monitoramento em nuvem que oferece visibilidade sobre o estado e o desempenho dos switches, disponível em https://www.datadoghq.com/product/network-monitoring/

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **Checkmk:** Uma solução de monitoramento de infraestrutura de TI que suporta o monitoramento de switches, fornecendo informações sobre taxas de pacotes, CPU, energia e largura de banda das portas, disponível em https://checkmk.com/
- **Auvik:** Uma ferramenta de gerenciamento de rede baseada em nuvem, projetada para MSPs (*Managed Service Provider*) e equipes de TI, com foco em descoberta automática, inventário e monitoramento de switches, disponível em https://www.auvik.com/

Ferramentas de Gerenciamento de Código Aberto

Essas ferramentas são gratuitas e contam com uma comunidade ativa para suporte e desenvolvimento.

- **Zabbix:** Uma solução de monitoramento de código aberto de nível empresarial, capaz de monitorar switches e outros dispositivos de rede. Oferece alertas personalizáveis e visualizações de dados flexíveis, disponível em https://www.zabbix.com/
- **Nagios Core/Nagios XI:** Uma ferramenta de monitoramento de código aberto amplamente utilizada, com uma grande comunidade e muitos *plugins* para monitorar switches via SNMP e outros protocolos. O Nagios, Figura 49, está disponível em duas versões:
    - **Nagios Core:** https://www.nagios.org/downloads/nagios-core/
    - **Nagios XI - Versão Comercial:** https://www.nagios.com/downloads/nagios-xi/

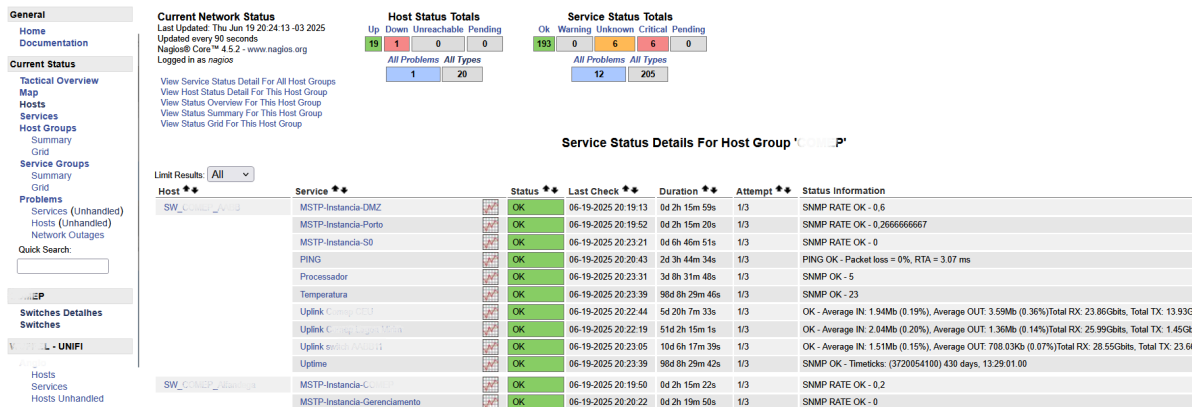


Figura 49. Ferramenta Nagios

- **LibreNMS:** Uma plataforma de monitoramento de rede de código aberto com foco em descoberta automática e suporte extensivo a dispositivos, é um *fork* da ferramenta Observium (https://www.observium.org/), incluindo switches, disponível em

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

https://www.librenms.org/ . Na Figura 50, a ferramenta Observium com switches sendo gerenciados por SNMP.

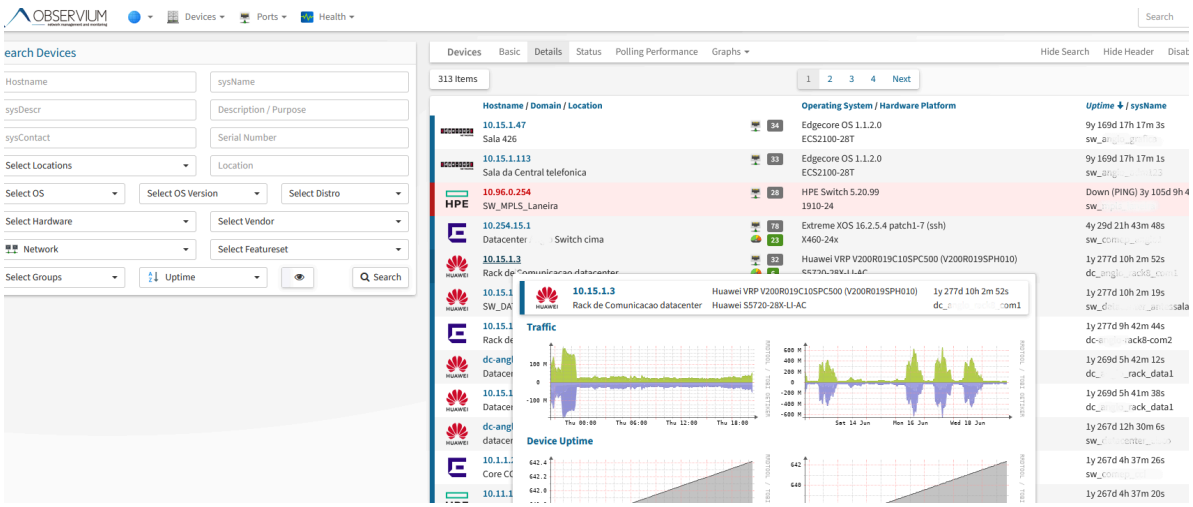


Figura 50. Ferramenta Observium

- **OpenNMS:** Uma plataforma de gerenciamento de rede de código aberto e de nível empresarial, com recursos para monitoramento de falhas e desempenho de switches, disponível em https://www.opennms.com/
- **Cacti:** Uma ferramenta de monitoramento de código aberto focada na visualização de dados através de gráficos, coletando informações de switches via SNMP, disponível em https://www.cacti.net/
- **Prometheus:** Um sistema de monitoramento de código aberto, popular em ambientes de nuvem e contêineres, que pode ser usado para monitorar métricas de switches, disponível em https://prometheus.io/

Observium - ferramenta de gerenciamento de redes (Parte 1) - https://youtu.be/afxzOHzT1tQ

Observium - ferramenta de gerenciamento de redes (Parte 2) - https://youtu.be/PGExnrKkLcg

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

7.7 Ferramentas de Simulação e Emulação

Uma alternativa interessante para aprendizado e resolução de problemas está no uso de ferramentas de simulação e emulação com switches gerenciáveis. Nestas ferramentas é possível montar cenários bem próximos aos reais de forma rápida e com possibilidade de variações que seriam bem complexas em ambiente real. Dentre as ferramentas mais aplicáveis em cenários com switches gerenciáveis, destacam-se:

- **Cisco Packet Tracer:** Desenvolvido pela empresa Cisco, é um simulador popular para estudantes e profissionais que buscam aprender sobre redes Cisco. Embora seja um simulador, o Packet Tracer oferece uma vasta gama de dispositivos de rede, incluindo switches, e permite a configuração de funcionalidades como VLANs, STP (*Spanning Tree Protocol*), *EtherChannel*, entre outras. A interface gráfica intuitiva e a capacidade de simular o fluxo de pacotes tornam excelente a ferramenta para visualizar o comportamento da rede e diagnosticar problemas em um ambiente controlado. Na Figura 51 um exemplo do ambiente da ferramenta Cisco Packet Tracer. Geralmente, o Cisco Packet Tracer é obtido através do cadastro e conclusão de um curso introdutório gratuito na Cisco Networking Academy (NetAcad): https://www.netacad.com/cisco-packet-tracer

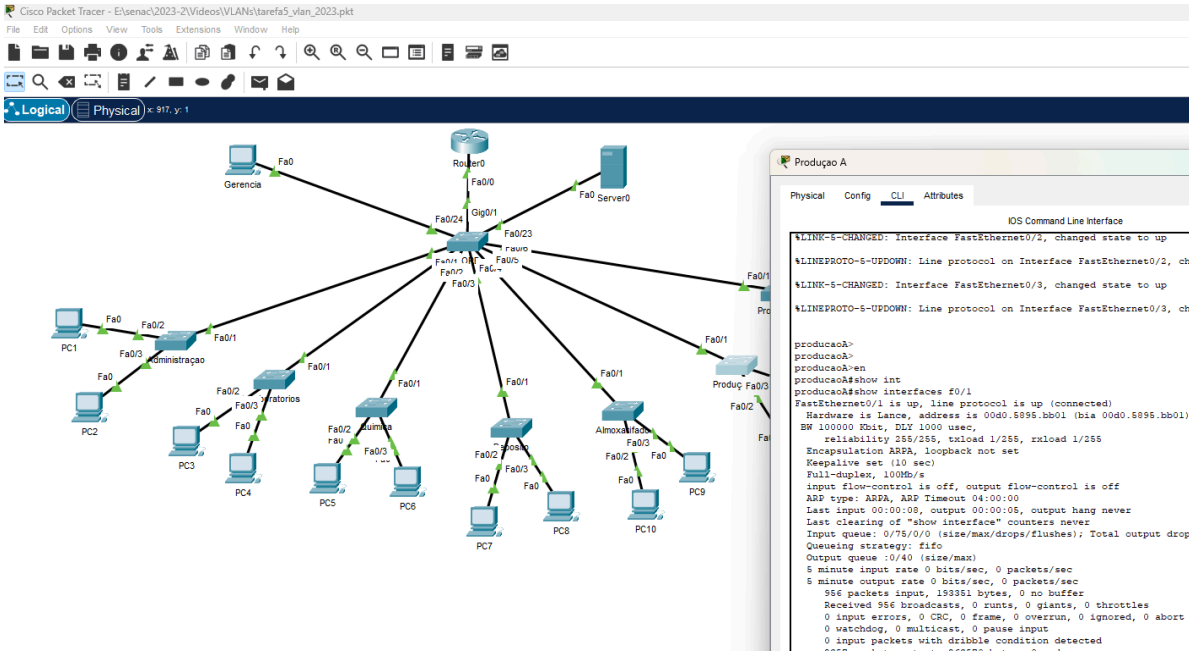


Figura 51. Um exemplo do ambiente da ferramenta Cisco Packet Tracer

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

- **GNS3 (Graphical Network Simulator-3):** O GNS3 é um emulador de rede em código-fonte aberto que se destaca pela sua capacidade de rodar imagens de sistemas operacionais reais de dispositivos de rede, como Cisco IOS, Juniper Junos e outros. Isso significa que o GNS3 não apenas simula, mas emula o comportamento do hardware, permitindo a configuração de funcionalidades avançadas de switches, incluindo recursos de Camada 2 (VLANs, STP, *Port Security*, DTP) e Camada 3 (SVIs, roteamento inter-VLAN, OSPF, EIGRP, etc.), com a mesma CLI (*Command Line Interface*) de um equipamento físico. A capacidade de integrar-se com máquinas virtuais (VMs) de hosts com sistemas operacionais diversos e outros dispositivos amplia ainda mais a fidelidade dos cenários. Na Figura 52 um exemplo do ambiente da ferramenta GNS3 e está disponível em https://www.gns3.com/software/download

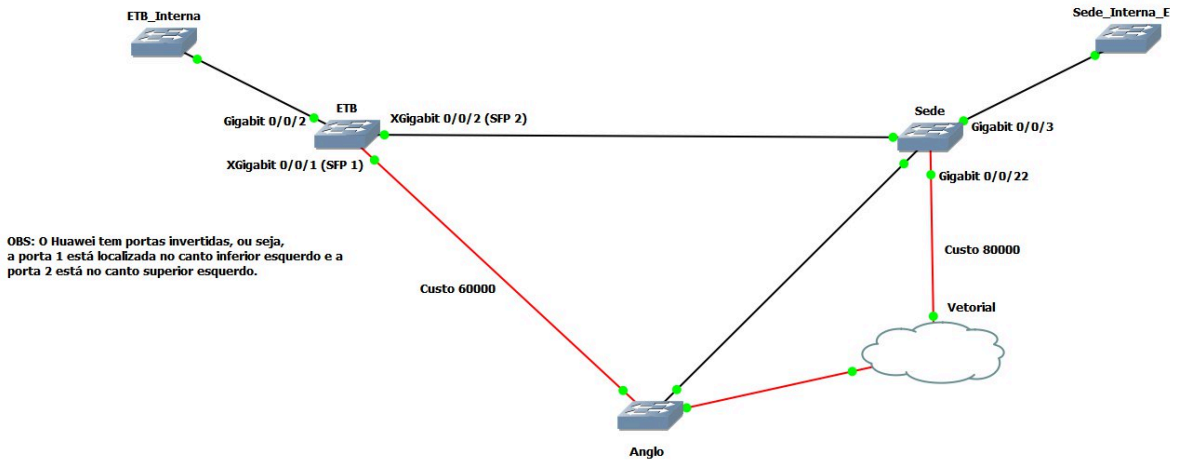


Figura 52. Um exemplo do ambiente da ferramenta GNS3

- **EVE-NG (Emulated Virtual Environment - Next Generation):** Semelhante ao GNS3, o EVE-NG é outra poderosa plataforma de emulação que suporta uma vasta gama de imagens de sistemas operacionais de diversos fabricantes (Cisco, Juniper, Palo Alto, Fortinet, etc.). A ferramenta oferece uma interface web mais moderna e colaborativa, permitindo que múltiplos usuários trabalhem no mesmo ambiente de laboratório. Para switches gerenciáveis, o EVE-NG suporta as mesmas funcionalidades avançadas de Camada 2 e Camada 3 que o GNS3, sendo uma escolha popular para estudos avançados, certificações e testes de interoperabilidade em ambientes heterogêneos. Está disponível em https://www.eve-ng.net/index.php/download/ , a versão *Community Edition* é gratuita. Na Figura 53 um exemplo do ambiente da ferramenta EVE-NG.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

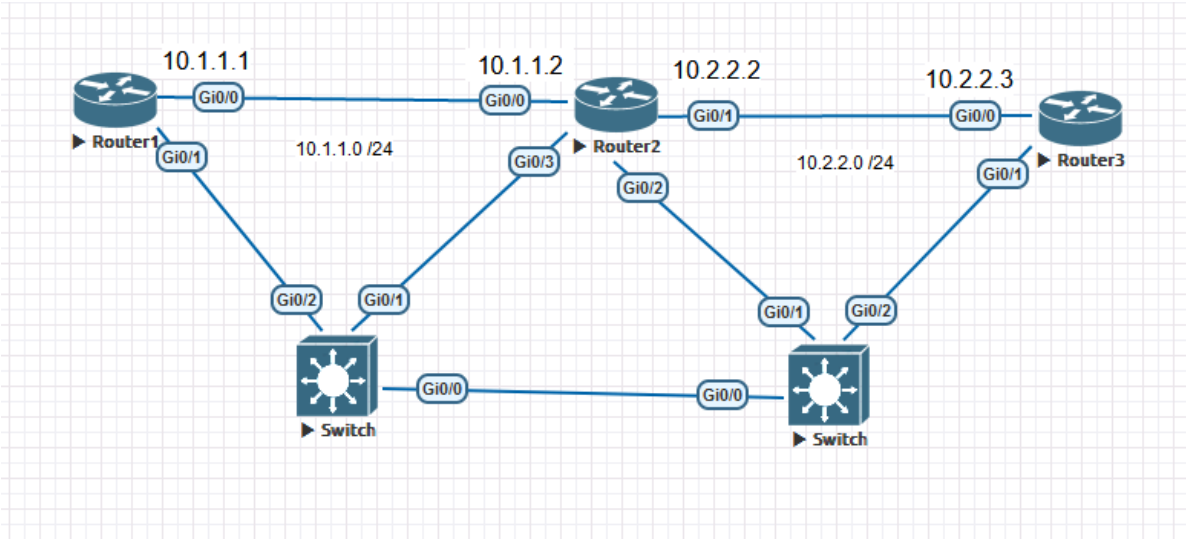


Figura 53. Um exemplo do ambiente da ferramenta Cisco EVE-NG

- **Huawei eNSP (Enterprise Network Simulation Platform):** Desenvolvida pela Huawei, a eNSP é a ferramenta oficial de simulação e emulação para seus próprios produtos de rede. Ela permite aos usuários criar e configurar topologias complexas com uma ampla variedade de dispositivos Huawei, incluindo routers (séries AR, NE), switches (séries S, CE), firewalls (USG) e dispositivos WLAN. A eNSP é particularmente valiosa para quem busca familiaridade com a sintaxe de comando (CLI) e as funcionalidades específicas dos equipamentos Huawei, oferecendo suporte a recursos avançados de *Layer 2* e *Layer 3*, como VLANs, STP, EtherChannel, OSPF, BGP, MPLS e VXLAN. É uma ferramenta indispensável para a preparação para as certificações Huawei (HCIA, HCIP, HCIE) e para o desenvolvimento de soluções que utilizam a tecnologia do fabricante. Na Figura 54 um exemplo do ambiente da ferramenta eNSP com um cenário simples. O *download* oficial da eNSP pode ser um pouco mais complexo devido às políticas de acesso da Huawei. Geralmente, é necessário ter uma conta no site de suporte da Huawei Enterprise. Procurar por "eNSP" na seção de softwares ou ferramentas. Para obter acesso ao eNSP, pode-se utilizar como ponto de partida utilizar o endereço https://support.huawei.com/enterprise/en/management-system/ensp-pid-9017384/software
    - *Observação: Às vezes, a Huawei restringe o download direto ou redireciona para parceiros/canais de educação. É possível que links de download de terceiros (como em blogs ou fóruns) existam, mas é sempre mais seguro obter a ferramenta de fontes oficiais.*

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

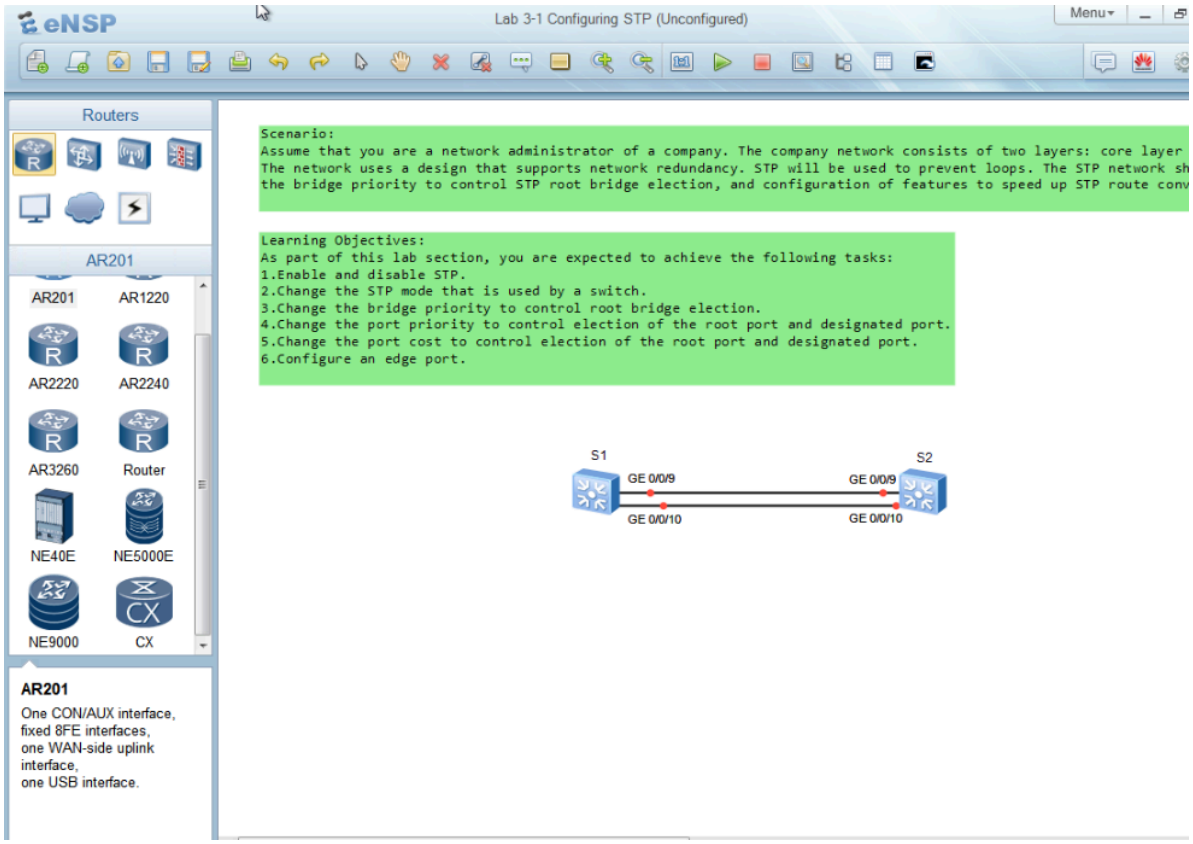


Figura 54. Um exemplo do ambiente da ferramenta eNSP

- **Mininet:** Voltado principalmente para redes definidas por software (SDN) e OpenFlow, o Mininet é um emulador de redes que cria uma rede de hosts, switches, controladores e links virtuais em uma única máquina. Embora seus switches nativos sejam OpenFlow-compatíveis e mais básicos em termos de funcionalidades de gerenciamento proprietárias, o Mininet é excelente para testar o comportamento de redes com controle centralizado e para entender como as VLANs podem ser programadas e gerenciadas por um controlador SDN. Pode ser complementado com imagens de switches mais complexos para cenários híbridos. Na Figura 55 um exemplo do ambiente da ferramenta Mininet. Disponível em http://mininet.org/download/

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

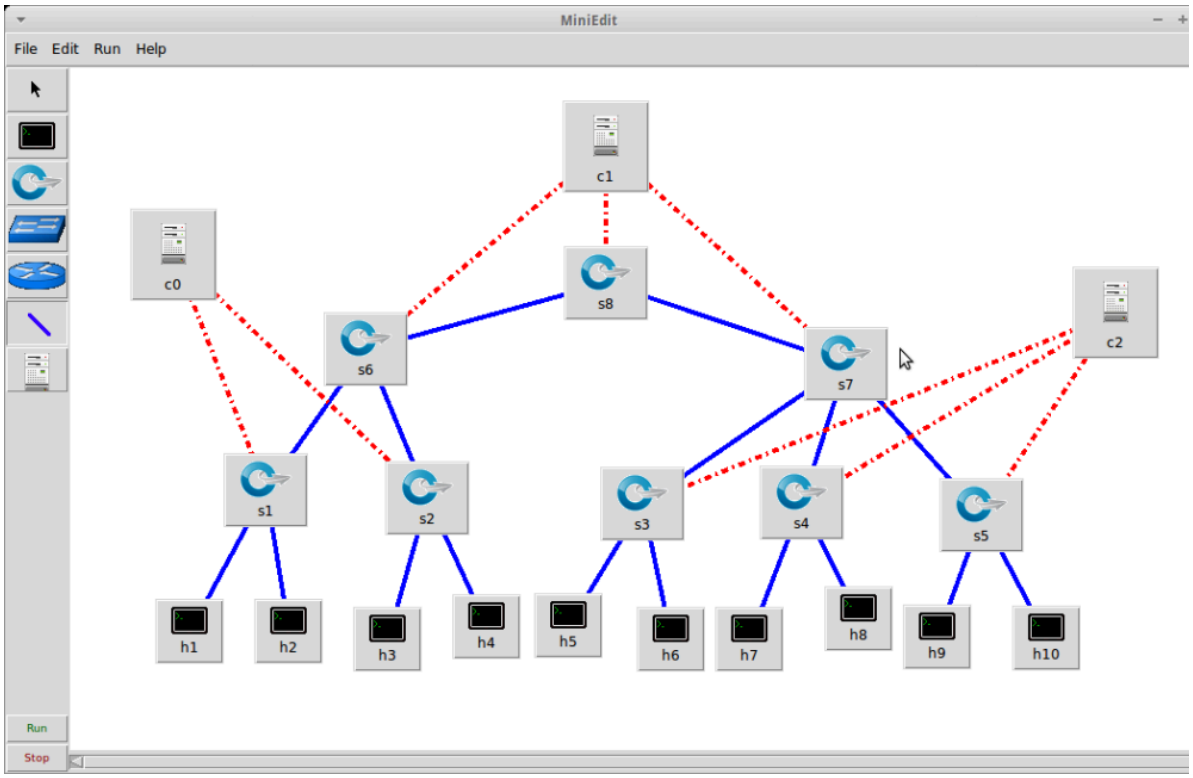


Figura 55. Um exemplo do ambiente da ferramenta Mininet

Redes para Iniciantes - Ferramentas de Aprendizagem - https://youtu.be/hF9VMircUbk

7.8 Boas Práticas

Para garantir a disponibilidade, a segurança e o bom desempenho da rede, a administração de switches gerenciáveis requer a adoção de boas práticas. Inicialmente, recomenda-se que o administrador de rede mantenha uma documentação detalhada de todos os switches. Isso inclui um inventário atualizado com informações como modelo, número de série, localização física, endereço MAC e IP de gerenciamento. A topologia da rede, ilustrando a interconexão entre os dispositivos, também deve ser documentada por meio de diagramas. Além disso, é essencial registrar as configurações específicas de cada switch, abrangendo VLANs, endereçamento IP, configurações de segurança (como ACLs e SNMP) e quaisquer ajustes de porta. Manter um histórico das alterações de configuração, com detalhes sobre quem realizou a modificação e quando, é igualmente importante. Para

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

isto podem ser usadas ferramentas de controle de versões tais como o Git (https://git-scm.com/).

No que diz respeito à configuração, sugere-se a utilização de convenções de nomenclatura consistentes para switches, VLANs e interfaces, facilitando a identificação e o gerenciamento. A implementação de configurações base para todos os switches, como servidores de log remoto, de NTP e de SNMP, garante uniformidade e simplifica o monitoramento. É aconselhável desabilitar portas não utilizadas para mitigar vulnerabilidades de segurança e evitar acessos indevidos. A configuração correta das velocidades e do modo *duplex* das portas é fundamental para prevenir problemas de desempenho.

Em termos de segurança, a primeira ação deve ser a alteração imediata das senhas padrão, utilizando credenciais com senhas fortes e complexas para acesso administrativo. Recomenda-se a utilização do protocolo SSH para acesso remoto seguro, em detrimento do Telnet. Em interfaces de administração web, a opção recomendada é para o uso do protocolo HTTPS ao invés do protocolo HTTP. O controle de acesso administrativo aos switches pode ser reforçado através da implementação de listas de controle de acesso (ACLs), permitindo apenas hosts ou redes confiáveis. A consideração da autenticação baseada em RADIUS ou TACACS+ para um gerenciamento centralizado de acesso é pertinente. A utilização do protocolo SNMPv3 com configurações de segurança robustas (autenticação e criptografia) é preferível em relação às versões mais antigas. A implementação de recursos de segurança de porta, como *Port Security* e STP, contribui para a prevenção de *loops* na rede e para o controle de acesso por endereço MAC. Manter o firmware dos switches atualizado é crucial para corrigir vulnerabilidades de segurança conhecidas.

Para um gerenciamento proativo, a implementação de um sistema de monitoramento de rede é essencial para acompanhar o estado e o desempenho dos switches. A configuração de alertas para eventos críticos, como falhas de conexão, alta utilização de recursos e erros de porta, permite uma resposta rápida a problemas. A análise regular dos logs dos switches auxilia na identificação de possíveis problemas ou atividades suspeitas. O monitoramento da utilização da largura de banda das portas é importante para identificar gargalos e planejar melhorias na capacidade da rede.

No gerenciamento de VLANs, o planejamento cuidadoso da estrutura é fundamental para segmentar a rede logicamente. A utilização de VLANs para isolar diferentes tipos de tráfego melhora a segurança e o desempenho. A documentação clara do propósito de cada VLAN e das portas a ela atribuídas é indispensável. O uso de uma VLAN de gerenciamento para administração dos dispositivos é fundamental para reduzir ao máximo a exposição a acessos não autorizados.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

A correta configuração do STP (*Spanning Tree Protocol*) e suas variações é vital para evitar *loops* na rede. A definição das *bridges root* primária e secundária em switches de maior capacidade (switches de *core*) garante a estabilidade da topologia. A utilização de recursos como *PortFast* e *BPDU Guard* nas portas de acesso melhora a convergência e previne problemas causados por dispositivos finais.

A realização de backups regulares das configurações dos switches é uma prática indispensável. Testar o processo de restauração garante a capacidade de recuperação em caso de falha ou erro de configuração. As cópias de backup devem ser armazenadas em um local seguro e separado dos switches Manter-se atualizado sobre as versões de *firmware* recomendadas pelo fabricante é importante para garantir o bom funcionamento e a segurança dos dispositivos. O planejamento e a execução de atualizações de *firmware* em janelas de manutenção minimizam o impacto na rede devido ao tempo consumido para realizar este procedimento. O monitoramento e a leitura das notas de modificações (*changelog*) do *firmware* antes da atualização é recomendada para entender as mudanças e os possíveis impactos.

O monitoramento da utilização dos recursos dos switches auxilia na identificação de possíveis gargalos de desempenho. O planejamento da capacidade da rede deve considerar as necessidades atuais e futuras. A escolha de switches com a capacidade de escalabilidade adequada é essencial para o crescimento da rede. Por fim, a realização de auditorias periódicas das configurações dos switches e das políticas de segurança implementadas, juntamente com a revisão regular da documentação da rede, garante que as práticas de administração permaneçam eficazes e alinhadas com as necessidades da organização.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Considerações Finais

Este livro foi concebido como um guia prático para a administração de switches gerenciáveis, compilado a partir de mais de 25 anos de experiência do autor na área. As dicas e procedimentos compartilhados são valiosos, visando contribuir para a melhoria das rotinas de administração de redes em ambientes corporativos. É importante compreender que as informações e sugestões apresentadas não são regras rígidas a serem seguidas como uma receita culinária, pois cada ambiente de rede possui particularidades que devem ser consideradas.

A melhor maneira de se desenvolver como um excelente profissional administrador de redes é através da experiência prática, que envolve experimentar, cometer erros e aprender com eles. No entanto, devido à diversidade inevitável de fabricantes e modelos de switches, a administração desses dispositivos pode se tornar complexa, mesmo existindo padrões e protocolos comuns. As interfaces de consoles de gerenciamento possuem formas proprietárias para execução de comandos e configurações. Diferentes modelos podem ter variações na configuração da porta de console, formatos de logs, procedimentos de restauração de fábrica, compatibilidade de *firmware* (até mesmo entre revisões de hardware do mesmo modelo), limitações em funcionalidades como espelhamento de portas e recursos computacionais para funções de *layer 3*.

Diante dessas particularidades de cada modelo de switch, o estudo constante e a exploração aprofundada da documentação específica fornecida pelo fabricante são essenciais para obter o melhor proveito dos switches gerenciáveis. A documentação é indispensável para confirmar configurações corretas (como parâmetros da porta de console e pinagem de cabos *rollover*), seguir procedimentos de instalação física, verificar atualizações de *firmware* recomendadas e realizar processos como backup/restore.

Além da experiência prática com os equipamentos e do estudo da documentação, o planejamento da infraestrutura da rede é fundamental para garantir a operação eficiente, confiabilidade e disponibilidade dos switches e da rede como um todo. Isso envolve a análise cuidadosa de fatores como a localização adequada para instalação física (considerando acessibilidade, umidade, poeira e temperatura), o planejamento do roteamento de cabos para evitar obstruções e facilitar expansões, a ventilação correta para dissipar calor, o fornecimento de energia estável e, idealmente, redundante com o uso de *nobreaks*, e a consideração da topologia da rede. O planejamento também é importante ao adicionar novos switches à rede, exigindo avaliação de necessidade, compatibilidade, topologia,

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

endereçamento e configuração inicial. A segmentação da rede com VLANs, baseada na aplicação ou disposição física dos hosts, também requer planejamento para otimizar o tráfego.

Para administrar switches gerenciáveis de forma eficaz, é fundamental dominar as funcionalidades básicas e saber onde e como aplicar as funcionalidades avançadas. As configurações avançadas são utilizadas em cenários de rede mais complexos, com maior quantidade de dispositivos, onde a administração demanda maior controle, segurança e desempenho. Os cenários típicos onde há maior demanda para o uso de switches gerenciáveis com funcionalidades avançadas são em redes locais corporativas.

As VLANs permitem a segmentação lógica da rede, isolando diferentes grupos de hosts por aplicação (como gerenciamento, voz, vídeo, servidores) ou localização, o que melhora a segurança e otimiza o desempenho. A implementação de VLANs requer um planejamento cuidadoso, incluindo a definição das identificações (VIDs), o agrupamento de hosts e o planejamento do endereçamento IP, associando-o aos VIDs para facilitar a administração e identificação. É importante associar as VLANs corretamente às portas de acesso (*untagged*) para dispositivos finais e às portas tronco (*tagged*) para interligação entre switches ou outros dispositivos que entendem a marcação

As ferramentas e os conhecimentos necessários para a resolução de problemas em switches gerenciáveis são fundamentais para que um administrador de redes obtenha sucesso. Isso envolve a capacidade de diagnosticar questões como dispositivos inacessíveis, VLANs que não funcionam, *loops* de rede e anomalias no comportamento do switch. As ferramentas de gerenciamento de rede e a análise de logs e estatísticas são indispensáveis para a identificação e solução proativa de problemas.

Em suma, para obter o máximo proveito dos switches gerenciáveis na administração de redes, a abordagem mais eficaz é uma combinação estratégica. Ela envolve a experimentação prática em bancada ou em ambientes controlados, o estudo dedicado das particularidades de cada modelo de switch por meio da documentação dos fabricantes, um planejamento robusto da infraestrutura de rede, o domínio das funcionalidades básicas e avançadas, o uso estratégico e planejado de VLANs, e a posse de ferramentas e conhecimentos para a resolução de problemas. Este livro teve como objetivo ser um facilitador nessa jornada, capacitando o leitor a alcançar um melhor desempenho na administração de redes com o uso de switches gerenciáveis.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional

Referências Bibliográficas

- ABNT. NBR 14565: procedimento básico para elaboração de projetos de cabeamento de telecomunicações para rede interna estruturada. Rio de Janeiro: ABNT, 2000.
- FILIPPETTI, Marco Aurélio. CCNA 4.1: guia completo de estudo. Rio de Janeiro: Visual Books, 2008.
- KUROSE, James; ROSS, Keith. Redes de computadores e a Internet: uma abordagem top-down. 3. ed. São Paulo: Pearson Education, 2007.
- LIMONCELLI, Thomas A. The Practice of System and Network Administration. 2. ed. EUA: Addison-Wesley Professional, 2007.
- MATTHEWS, J. Rede de Computadores: protocolos de Internet em Ação. Rio de Janeiro: LTC, 2006.
- MOTA FILHO, João Eriberto. Análise de Tráfego em Redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional. São Paulo: Novatec, 2013.
- ODOM, Wendell. CCNA ICND 2 Guia Oficial de Exame. 2. ed. Rio de Janeiro: Alta Books, 2008.
- OPPENHEIMER, Priscilla. Top-Down Network Design. 2. ed. EUA: Cisco Press, 2004.
- PETERSON, Larry; DAVIE, Bruce. Redes de Computadores. 3. ed. Rio de Janeiro: Campus, 2004.
- PINHEIRO, José Maurício S. Cabeamento óptico. Rio de Janeiro: Campus, 2003.
- PINHEIRO, José Maurício S. Guia completo de cabeamento de redes. Rio de Janeiro: Campus, 2003.
- SANDERS, Chris. Análise de pacotes na prática. São Paulo: Novatec, 2017.
- SHIMONSKI, Robert. Wireshark Guia Prático: análise e resolução de problemas de tráfego em rede. São Paulo: Novatec, 2013.
- SILBERSCHATZ, A.; GALVIN, P. B. Fundamentos de Sistemas Operacionais. 6. ed. São Paulo: LTC, 2004.
- SOARES, L. F. Gomes. Redes de computadores das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.
- TANENBAUM, Andrew S. Redes de computadores. Rio de Janeiro: Campus, 2003.
- TRULOVE, James. LAN Wiring. 3. ed. EUA: McGraw-Hill, 2005.

Este trabalho está licenciado com uma Licença Creative Commons - Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional